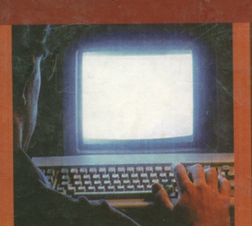
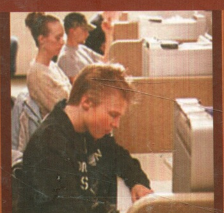
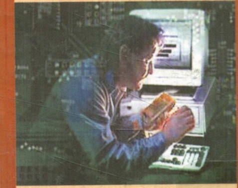
دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت

وجرائم الاحتيال المنظم باستعمال شبكة الانترنت

الحماية الجنائية للبرامج بمقتضى قانون حق المؤلف - الحماية الجنائية لبراءة الاختراع - الصعوبات القانونية المتعلقة بتطبيق أحكام السرقة على جرائم الكمبيوتر - الصعوبات القانونية المتعلقة بإعمال قواعد النصب في مجال الكمبيوتر والانترنت - ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات الاختصاص الدولي بمحاكمة المتهمين بجرائم الانترنت - خصائص الاحتيال المنظم







دكتور
غنام محمد غنام
أستاذ ورئيس قسم القانون الجنائى
كلية الحقوق جامعة المنصورة

دار الفكر والقانون
اشارع الجلاء - أمام بوابة الجامعة
المنصورة - برج آية
تليفون : ٠٥٠٢٢٩٠٨٩٨ - محمول : ٠١٠٦٠٥٧٧٦٨

دور قانون العقوبات

في مكافحة جرائم الكمبيوتر والانترنت

وجرائم الاحتيال المنظم باستعمال شبكة الانترنت

الحماية الجنائية للبرامج بمقتضى قانون حق المؤلف – الحماية الجنائية لبراءة الاختراع – الصعوبات القانونية المتعلقة بتطبيق أحكام السرقة على جرائم الكمبيوتر – الصعوبات القانونية المتعلقة بإعمال قواعد النصب في مجال الكمبيوتر والانترنت – ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات – الاختصاص الدولي بمحاكمة المتهمين بجرائم الانترنت – خصائص الاحتيال المنظم

دكتور
غنام محمد غنام
أستاذ ورئيس قسم القانون الجنائي
كلية الحقوق – جامعة المنصورة

طبعة ٢٠١٠

دار الفكر والقانون
المنصورة
ت : ٠٥٠/٢٢٩٠٨٩٨
محمول : ٠١٠٦٠٥٧٧٦٨

دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت

المؤلف : د. غنام محمد غنام

رقم الإيداع بدار الكتب المصرية : ٢٣٧٩٢

سنة الطبع ٢٠١٠

الترقيم الدولي : .I.S.B.N

978-977-6253-26-1

الإخراج الفني: مطابع أبو الخير - الاسكندرية

دار الفكر والقانون

للنشر والتوزيـــع

١ ش الجلاء أمام بوابة الجامعة برج آية

تليفاكس : ٠٠٢٠٥٠٢٢٣٥٦٧١ تليفون : ٠٥٠٢٢٩٠٨٩٨

محمول ٠٠٢٠١٠٦٠٥٧٧٦٨

المحامي / أحمد محمد أحمد سيد أحمد

يتناول هذا الكتاب بين دفتيه ثلاثة موضوعات يظهر من خلالها التحديات التي يثيرها التقدم التقني في مجال المعلومات للقواعد التقليدية في قانون العقوبات وفي قانون الإجراءات الجنائية. هذه الموضوعات الثلاثة هي: دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت.

(وسوف ندرسه في الباب الأول).

ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات.

(وسوف نعالجه في الباب الثاني).

الاحتيال المنظم باستعمال شبكة الإنترنت

(وسوف نفرد له الباب الثالث).

وقد اخترتنا تلك الموضوعات الثلاثة لأنها تبرز الجوانب الموضوعية والإجرائية التي تتميز بها جرائم المعلوماتية.

الباب الأول

دور قانون العقوبات

مكافحة جرائم الكمبيوتر والإنترنت

١- موضوع الدراسة :

يعالج هذا الباب موضوع جرائم الحاسب الآلي (الكمبيوتر) للتعرف على دور قانون العقوبات في مواجهة هذا النوع الحديث من الجرائم. فقد ظهر في الآونة الأخيرة هذا النوع التقني من الجرائم والذي يصعب أحيانا تحديد الطائفة التي ينتمي إليها ، هل هي من جرائم الأموال أو هي من جرائم الأشخاص أو من جرائم المصلحة العامة ؟ كما يصعب أحيانا تحديد هوية هذا النوع من الإجرام : هل هو من الجرائم التقليدية أو من الجرائم الاقتصادية أو أنه لا ينتمي إلى هذا أو ذاك وأنه من نوعية جديدة من الجرائم؟

وقد ظهرت التحديات التي تثيرها جرائم الكمبيوتر في البلاد الصناعية المتقدمة التي سبقت في مجال استخدام هذا النوع من الأجهزة . فقد تلازم ظهور الحاسب الآلي في هذه البلاد مع خطورة اجتماعية على عدة مصالح يتعين التدخل لحمايتها بطريق القانون الجنائي . فقد أدركت كثير من البلاد (الولايات المتحدة وأوربا) أنه لا يكفي الاستعانة بطرق الحماية المدنية للحفاظ على كثير من المصالح التي يهددها هذا النوع من الجرائم . وتعود أول تشريعات مكافحة جرائم الكمبيوتر في الولايات المتحدة الأمريكية إلى سنة ١٩٧٨ حيث صدر قانون بهذا الخصوص في ولاية فلوريدا Florida وفي ولاية أريزونا Arizona ، وعلى المستوى الفيدرالي صدرت أول

التشريعات الأمريكية في سنة ١٩٨٤ [1] .

في مواجهة هذه التحديات توسل قانون العقوبات بطرق تقليدية مستقرة لمواجهة جرائم الحاسب الآلي ، مثل تلك المقررة في جرائم الأموال (السرقة والنصب وخيانة الأمانة) ، ومثل تلك المقررة في جرائم المصلحة العامة (جرائم التزوير). بيد أنه قد تبين قصور هذا الوسائل التقليدية عن مواجهة العديد من الأفعال التي تهدد مصالح اجتماعية والتي ارتبطت بظهور وانتشار أجهزة الحاسب الآلي ، على نحو ما سيؤكده هذا البحث .

فقد تبين في بعض الأحوال أن ثمة أفعالا جديدة ترتبط باستعمال الحاسب الآلي لا تكفي النصوص القائمة لمكافحتها ، من ذلك الاعتداء على حرمة الحياة الخاصة. هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلاّ إذا كان مرتبطا بمكان خاص. أما تجميع معلومات عن الأفراد وتسجيلها في الكمبيوتر ، فإنه لا يخضع للتأثيم وفقا للقواعد العامة . كما أن التداخل في نظام الحاسب الآلي وتغيير البيانات تشكل صورا جديدة لا يعرفها قانون العقوبات قبل ظهور الحاسب الآلي نفسه . كل ذلك يؤكد قصور القواعد التقليدية في القانون الجنائي عن مكافحة هذا النوع الجديد من الجرائم .

وقد كان ذلك هو السبب في أن كثيرا من البلاد أدخلت تشريعات جديدة تعالج جرائم الكمبيوتر على وجه الخصوص. من هذه البلاد الولايات المتحدة الأمريكية والدول الأوربية . كما أصبح من الضروري مراجعة القواعد التقليدية لمواءمتها مع الحاجة المتجددة بسبب ظهور وانتشار

---

(١) انظر

Edward M. Wise , Computer Crimes and Other Crimes against Information Technology in the United States , Rev.int.dr.pén.1993,p.657.

الكمبيوتر. من هذه القواعد التقليدية ما يتعلق بمفهوم المال في جرائم الأموال وبسرقة المنافع وبسرقة الوقت وبمفهوم الركن المعنوي في جرائم الأموال وبمفهوم المحرر في جرائم التزوير .

وعلى الرغم من الحاجة إلى مراجعة القواعد الجنائية التقليدية لمواجهة جرائم الحاسب الآلي ، وعلى الرغم من سن التشريعات الخاصة لمواجهة صور معينة من هذه الجرائم ، فإن المشرع في البلاد العربية لم يستشعر بعد الحاجة إلى التدخل لمواجهة هذا النوع من الجرائم بنصوص خاصة . كما أن القضاء لم يواجه بعد بمشكلات قانونية تتعلق بحماية المعلومات والبرامج التي تخص الحاسب الآلي. ويُثار التساؤل عن سبب هذه الظاهرة الذي يبدو أنه يكمن في ضعف النشاط التجاري في البلدان العربية بالمقارنة بما هو عليه الحال في البلاد الغربية . ولا ننسى أن كثيرا من الإدارات العامة لا تزال تحفظ معلوماتها على ملفات من ورق، ويخالج المسؤولين الشك حول الاعتماد كلية على الكمبيوتر في تخزين تلك المعلومات. يضاف إلى ذلك أن برامج الحاسب الآلي تم إعدادها في الخارج، وهو الأمر الذي لا يحث البلاد العربية على الإسراع بحماية تلك البرامج ، لأن ذلك من شأنه أن يعمل على رفع أسعار تلك البرامج .

٢- المقصود بالكمبيوتر:

يقصد بالكمبيوتر كل آلة تقوم بمعالجة البيانات بطريقة آلية. ويقصد بالمعالجة تخزين هذه البيانات ، سواء في داخل الجهاز نفسه، أو على دعامة مادية أخرى ممغنطة. كما أن هذا التخزين لا يكون كذلك إلاّ إذا سمح للمتعامل مع هذا الجهاز بالرجوع إليه ومراجعة تلك البيانات .

وتحرص بعض التشريعات على إيراد تعريف للكمبيوتر في مفهوم

جـرائم الكمبيـوتر. ويرجـع ذلـك إلى أن كـثيرا مـن الآلات تـسير الآن بالكمبيوتر، فالآلات الحاسبة وماكينات الطباعة والأدوات المنزلية يعمل كثير منها بالكمبيوتر، ومع ذلـك فإنهـا لا تـدخل في مجـال جـرائم الكمبيـوتر في مفهوم هذا البحث[١].

ومن التشريعات التي تهتم بتعريف الكمبيوتر التشريع الكندي الـذي حدد مفهومه بأنه "جهاز أو أكثر تتصل فيما بينها تقوم بوظيفة أو أكثـر مـن الوظائف التالية: (أ) تشغيل بـرامج أو معلومـات معالجـة آليـا، (ب) تقـوم بالوظائف التالية تطبيقا لبرامج معينة : ١- تنفيذ عمليات منطـق وسـيطرة ، ٢- تنفيذ أي وظيفة أخرى"[٢]. وعرّف قـانون جـرائم الكمبيـوتر في ولايـة فلوريدا الأمريكية الكمبيوتر بأنه آلة مبرمجة داخليـا وتعمـل بطريقـة تلقائيـة لمعالجة البيانات[٣]. ويعرفه قـانون جـرائم الكمبيـوتر في ولايـة Tennessee بالولايات المتحدة الأمريكية بأنه آله تقوم بعمليـات المعالجـة مـشتملة علـى عمليات رقمية ورياضية ومنطقية دون تدخل مـن الغـير في أثنـاء أداء ذلـك العمل[٤]. ويعرفه قانون جرائم الكمبيوتر في ولاية فرجينيا Virginia لـسنة ١٩٨٤ بالولايـات المتحـدة الأمريكيـة بأنـه آلـة أو مجموعـة مـن الآلات الإلكترونية و المغنطيسية الهيدروليكية أو العضوية التي تعمل وفقا لبرنامج أو تبعا لتعليمات مسبقة من شخص وتعمل بطريقة تلقائية منفذة عمليات محلها

---

(1) Donald K. Piragoff, Computer Crimes and Other Crimes against Information Technology in Canada , Rev.int.dr.pén.1993,p.224.

(٢) ينص الفصل رقم ٣٤٢/ ١ من قانون العقوبات الكندي على أن : computer system means a device that , or a group of interconnected or related devices one or more of which
(a) contains computer programs or other data , and
(b) pursuant to computer programs ,
(i) performs logic and control , and
(ii) may perform any other function " .

(٣) انظر تعريف ذلك في قانون جرائم الكمبيوتر في ولايـة فلوريـدا الأمريكيـة (فـصل رقـم ٨١٥) :

Computer means an internally programmed, automatic device that performs data processing.

(٤) انظر التعريف الوارد في هذا القانون

Computer " means a device that can perform substantial computing , including numerous arithmetic or logic operations , without intervention by a human operator during the processing of a job " .

بيانات معينة أو بالاستعانة بتلك البيانات ويمكنها أن ترسل النتائج إلى شخص أو إلى جهاز آخر . وينسحب وصف الكمبيوتر وفقا لهذا القانون على كل جهاز يقوم بمساعدة الكمبيوتر على أن يقوم بتخزين أو استعادة أو إرسال بيانات أو برامج من أو إلى شخص آخر أو إلى جهاز كمبيوتر آخر(١)

ولا يقتصر مفهوم البيانات على ما هو مكتوب فقط ، بل يشكل كل ما يتم تصويره أو رسمه من أشكال مختلفة . وبناء عليه فإن الصور المختلفة للألعاب والتي تقوم بعض " أجهزة الفيديو جيم" بتقديمها serveurs télématiques تدخل في عداد الكمبيوتر (٢) .

وعلى الرغم من ذلك فإن تعبير " كمبيوتر " يستخدم أحيانا لينسحب على آلات لا تعالج بيانات ، مثل آلات سحب النقود في البنوك و المفكرات الإلكترونية الشخصية (٣) .

وتحدد بعض التشريعات المقصود بشبكة الكمبيوتر Computer Network. فيعرفها قانون ولاية Tennessee بأنها تتكون من جهازين أو

---

(١) انظر قانون جرائم الكمبيوتر في ولاية فيرجينيا Virginia :

" Computer means an electronic , magnetic, optical , hydraulic or organic device or group of devices which, pursuant to a computer program , to human instruction , or to permanent instructions contained in the device or group of devices , can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person . The term " computer " includes any connected or directly related device , equipment , or facility which enables the computer to store , retrieve or communicate computer programs, computer date or the results of computer operations to or from a person , another computer or another device " .

2))Trib. corr. de Paris 5 nov. 1996, Expertises, n° 202, fév. 1997, p. 81; Cahiers Lamy droit de l'informatique , Bulletin d'actualité, n° 89 fév. 1997,p. 9 et 10 .

(٣) انظر

Marise Cremona , Jonathan Herring Ma , Criminal law , Macmilan, 1998, p. 234 : " has been held to include machines which are not normally reffered to as a computer, such as electronic personal organisers or cash registers . "

(٢) انظر قانون في شأن جرائم الكمبيوتر في ولاية Tennessee حيث يعرف الشبكة بأنها :

"Computer network means a set of two or more computer systems that transmit data over communication circuits connecting them "

أكثر من أجهزة الكمبيوتر ترتبط فيما بينها بدائرة لنقل البيانات [1] . ولا يخرج قانون ولاية فيرجينيا عن هذا المعنى [2] . فقد عرّف هذا القانون الشبكة بأنها اتصال بين أكثر من جهاز كمبيوتر بشكل يتيح تبادل البيانات بين هذه الأجهزة .

وعلى العموم فإن الرأي الراجح يتجه إلى أن النصوص التي تحمي نظام الكمبيوتر تسري أيضا على الاتصال بين أنظمة (أجهزة) الكمبيوتر عند تعددها[3] .

وكان الاتجاه سائدا في فرنسا لتعريف النظام باشتراط أن يكون محميا بنظام للأمان ، فعرفه مقرر مجلس الشيوخ عند إعداد قانون سنة ١٩٨٨ بأنه " مجموع مركب من وحدة أو أكثر من المعالجة ، والذاكرة ولعناصر للإدخال والإخراج وعلاقة بين تلك العناصر تتكامل فيما بينها نحو نتيجة معينة، وهذا المجموع يحميه نظام للأمان "([4]) . وقد تم التخلي في وقت لاحق عن هذا الشرط الأخير المتعلق بضرورة إحاطة النظام بوسيلة أمنية (كلمة السر مثلا) حتى يتمتع بصفة النظام محل الحماية الجنائية .

وفي نفس الاتجاه يعرف قانون "الكمبيوتر والحريات" في فرنسا لسنة ١٩٧٨ (١٥ يناير) معالجة الكمبيوتر للمعلومات ، وذلك في خصوص

---

(٢) انظر قانون في شأن جرائم الكمبيوتر في ولاية فيرجينيا حيث يعرف الشبكة بأنها :

" Computer network means a set of related , remotely connected devices and any communications facilities including more than one computer with the capability to transmit data among them through the communications facilities " .

(٣) انظر :

Guillaume CHAMPY, La fraude informatique , Presses Universitaires d'Aix-Marseille , 1992, p. 140 .

(٤) مشار إليه في :

Guillaume CHAMPY, La fraude informatique, Presses Universitaires . 1992 , p. 122.

مجال تطبيق هذا القانون الذي يفرض التزامات معينة - بخصوص تجميع البيانات الشخصية - بأنها " مجموع من العمليات يتم تنفيذها بوسائل آلية تتعلق بتجميع وتسجيل وإعداد و تعديل وحفظ وحذف المعلومات الاسمية ، كما تتضمن مجموعا من العمليات من نفس الطبيعة والتي تتعلق باستغلال الفيش وقاعدة البيانات "(مادة ٥)[١].

٣- المقصود بجرائم الكمبيوتر:

نقصد بجرائم الكمبيوتر هنا جرائم الأموال وجرائم الأشخاص وجرائم المصلحة العامة التي تقع باستعمال الكمبيوتر. كما نقصد بجرائم الإنترنت تلك الجرائم التي تقع عن طريق استعمال شبكة الإنترنت سواء داخل البلاد أو خارجها.

وقد عنيت بعض التشريعات بالتسوية بين الكمبيوتر والآلات التي يتم تشغيلها بواسطة عملة نقدية أو ماركة أو كارت. من ذلك قانون العقوبات الأسترالي بعد تعديله في سنة ١٩٨٥ الذي تضمن الفصل رقم ١١٥ منه ذلك الحكم[٢] .

٤- مدى خطورة جرائم الحاسب الآلي والإنترنت:

كشف الانتشار الواسع في استخدام أجهزة الكمبيوتر عن خطورة ترتبط بهذا النوع من الاستخدام على عدة مصالح اجتماعية ومصالح فردية يهم المجتمع حمايتها . فما لبث أن زاد استعمال الحاسب الآلي إلى الحد الذي

---

(1) " Est dénommé traitement automatisé d'informations nominatives au sens de la présente loi, tout ensembe d'opérations réalisées par des moyens automatiques , relatif à la collecte, l'enregistrement, l'élaboration , la modification , la conservation et la destruction d'informations nminatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données ... " .
(2) secton 115 , subsection 2 .

أصبح فيه لا غنى عنه لسير الحياة في المجتمع . فقد غير معالم النشاط الاقتصادي والتجاري والثقافي والعلمي ، بل ونشاط الأفراد في حياتهم الخاصة. هذا التوغل في حياة الفرد والمجموع برهن بجلاء عن ظهور قيم جديدة ترتبط بهذا الجهاز ، منها ضرورة الحرص عليه وحمايته من العدوان. فالعدوان على أنظمة الكمبيوتر يمكن أن يهدد الحياة بالشلل . بل إنه ليس من المغالاة أن نقول إن العبث بأنظمة الكمبيوتر يمكن أن يهدد الأمن والسلم الدولي ، حيث إن كثيرا من الأسلحة ، ومنها النووية ، مرتبط في انطلاقه بأنظمة الكمبيوتر.

والحقيقة أن ضرورة حماية أنظمة الكمبيوتر ليس الغرض منها حماية الجهاز كقيمة اجتماعية مستقلة ، وإنما الغرض هو حماية المصالح العامة والمصالح الخاصة التي يحميها المجتمع والتي ترتبط باستعمال الحاسب الآلي . فالمعلومات المبرمجة ملك لصاحبها . وبالتالي فإن حمايتها هي حماية للملكية من العبث بها في صورة استيلاء أو اطلاع أو إتلاف . كما أن حمايتها حماية للمستندات التي تخرج عن هذا الجهاز . وبالتالي فإن حماية نظام الكمبيوتر هي حماية للثقة العامة في المحررات.

غير أنه تبين أن نظام الحاسب الآلي وما يرتبط به من استعمال شبكة الإنترنت له دور إجرامي، إي أنه يسهل ارتكاب أنواع معينة من الجرائم . ومؤدى ذلك أن نظام الحاسب ليس دائما الضحية ولا هو محل للعدوان ، بل هو وسيلة الجاني في بعض الأحوال. من ذلك جرائم بث الأفلام والصور الفاضحة ، أو ارتكاب جرائم ضد أمن الدولة أو ضد الأديان . ومن ذلك أيضا ما تقوم به أنظمة الحاسب من تسهيل جرائم السرقة والنصب والاستيلاء على أموال البنوك وغيرها من الشركات.

٥- عدم تطور قوانين الكمبيوتر والإنترنت:

على الرغم من تطور أجهزة الكمبيوتر وظهور وتطور شبكة الإنترنت، فإن القوانين التي تنظم هذا النوع من النشاط لم يتم إعدادها بالشكل الملائم الذي يكفل مواجهة هذا التطور التقني المستمر. ولا ننسى أن البلاد العربية لم تعرف من التشريعات ما يعالج هذا النوع من النشاط .

يُضاف إلى ذلك أن استعمال شبكة الإنترنت لا يزال يحتاج إلى وضع نظام قانوني ملائم يأخذ في الاعتبار الطبيعة الدولية لتلك الشبكة . كما يستلزم ذلك وضع تنظيم أفضل للتعاون الدولي في هذا المجال .

٦- السمات العامة للمجرم المعلوماتي:

تسود تفرقة تقليدية في دراسات علم الإجرام تقوم على التمييز بين الإجرام الطبيعي والإجرام الاصطناعي نادى بها الإيطالي جاروفالو . فهل ينتمي المجرم المعلوماتي إلى النوع الأول من الإجرام أم ينتمي إلى النوع الثاني؟ الحقيقة أن المجرم المعلوماتي تعبير ينطوي على قدر من التجاوز في القول. فمن الصحيح القول بأنه لا يوجد نموذج محدد للمجرم المعلوماتي، بل إن هناك عدة نماذج للمجرمين قد يستخدمون الكمبيوتر في جرائمهم وقد يقومون بأفعال إجرامية ضد نظام الكمبيوتر نفسه. فهناك من يسرق النقود من البنك بالاستعانة بأنظمة الكمبيوتر، وهناك من يتحايل على الكمبيوتر بالاستعانة بالكمبيوتر أي بجهاز آخر للكمبيوتر يصدر منه أمر إلى الجهاز الأول لتحويل أموال على حساب له قد قام بفتحه أيضا بالتحايل على كمبيوتر ثالث. وهناك من يرتكب جريمة تزوير بالاستعانة بالكمبيوتر وذلك بتعديل البيانات المحفوظة فيه والتي يتم إخراجها في شكل محررات ورقية بعد ذلك. وهكذا الأمر بالنسبة لصور أخرى من الجرائم. وبالتالي ترجع الصعوبة في تحديد خصائص معينة للمجرم المعلوماتي إلى تعدد جرائم الكمبيوتر وتنوعها لكي تغطي صورا عديدة من الأنشطة.

وعلى الرغم من ذلك فإنه يمكن القول بوجود قاسم مشترك بين هؤلاء المجرمين يؤكد أنهم ينتمون إلى المجرمين ذوي الياقات البيضاء. وليس معنى ذلك أنهم أقل خطورة من الناحية الإجرامية عن المجرمين ذوي الياقات الزرقاء ، بل يعني ذلك أنهم يختلفون عنهم في اتجاهات شخصياتهم . وعلى الرغم من انتمائهم بوجه عام إلى المجرمين ذوي الياقات البيضاء فإنهم طائفة متميزة عنهم تتخصص في جرائم الكمبيوتر . فهم إما يقومون بالاعتداء على أجهزة الكمبيوتر أو يقومون الاستعانة بالكمبيوتر في ارتكاب جرائمهم .

ويمكن إجمال أهم سمات المجرم المعلوماتي في الآتي :

١ – المجرم المعلوماتي مجرم متخصص :

ثبت من عديد من القضايا أن عددا من المجرمين لا يرتكبون إلاّ جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم .

٢ – المجرم المعلوماتي مجرم عائد إلى الإجرام أحيانا :

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة. ويؤدي ذلك إلى العود إلى الإجرام. وقد ينتهي بهم الأمر في المرة التالية إلى تقديمهم إلى المحاكمة .

٣ – المجرم المعلوماتي مجرم هاو في حالات كثيرة :

لا يسهل على الشخص الهاوي، إلاّ في حالات قليلة ، أن يرتكب جرائم بطريق الكمبيوتر، فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما يحدث في البنوك مثلا .

ولا يحول ذلك دون ظهور مجرمين هواه في مجال هذا النوع من الجرائم في حالات عديدة. وهذا ما أثبتته أحداث كثيرة في بلاد متعددة وخاصة في الولايات المتحدة الأمريكية .

٤ – المجرم المعلوماتي مجرم ذكي:

لا يمكن أن ينتمي المجرم المعلوماتي إلى طائفة المجرمين الأغبياء . فإذا كان من يسرق من منزل أو من سيارة منخفض الذكاء في كثير من الأحيان، فإن من يستعين بالكمبيوتر في السرقة من أموال بنك أو شركة يتميز بمستوى مرتفع من الذكاء حتى يستطيع أن يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته. فهو أقرب إلى مرتكبي جريمة النصب منه إلى مرتكبي جريمة السرقة.

٥ –المجرم المعلومات مجرم غير عنيف:

ينتمي الإجرام المعلوماتي إلى إجرام الحيلة، فلا يلجأ المجرم المعلوماتي إلى العنف في ارتكاب جرائمه. هذا النوع من الجرائم لا يستلزم مقدارا من العنف للقيام به.

٦ – المجرم المعلوماتي متكيف اجتماعيا:

لا يضع المجرم المعلوماتي نفسه في حالة عداء سافر مع المجتمع الذي يحيط به. بل إنه إنسان متكيف معه. ذلك أنه أصلا إنسان مرتفع الذكاء. ويساعده ذلك على عملية التكيف ، وما الذكاء في رأي كثيرين سوى القدرة على التكيف. ولا يعني ذلك التقليل من شأن المجرم المعلوماتي ، بل إن خطورته الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه .

٧- أهمية موضوع البحث:

تبدو أهمية البحث من خلال أهمية موضوعة على ما سلف بيانه. ويرجع ذلك بصفة خاصة إلى توغل أجهزة الحاسب الآلي في حياة الفرد وفي حياة المجتمع وفي أنشطة المجتمع الدولي. فلم يعد ثمة مجال للاستغناء عن جهاز الحاسب. ومن ثم كانت الرغبة في حماية أنظمة هذا الجهاز من الناحية الجنائية ومن الناحية المدنية وكذلك من الناحية الإدارية. كما ظهرت الحاجة إلى حماية الفرد من تسلط هذا الجهاز وما يمثله من خطورة على قيم اجتماعية أساسية من الحق في الملكية والحياء العام وغيرها.

وتبدو الأهمية العلمية للبحث في مجال جرائم الكمبيوتر إلى استطلاع ما توصل إليه الآخرون في مكافحة جرائم الكمبيوتر، وذلك حتى نبدأ من حيث انتهى إليه الآخرون، وحتى نكون على استعداد لسن تشريعات مناسبة عندما يستشعر المشرع الحاجة إلى ذلك.

٨- المشكلات القانونية التي يثيرها موضوع البحث:

يصبو هذا البحث إلى إيجاد إجابة لبعض الأسئلة التي ترتبط بجرائم الكمبيوتر، من أهم هذه الأسئلة: لماذا لا تكفي القواعد التقليدية في القانون الجنائي لمواجهة جرائم الكمبيوتر ؟ ما هو حجم التعديلات التي يتعين إدخالها حتى تتم ملاءمة تلك القواعد لتلك النوعية من الجرائم ؟ هل يلزم التدخل بنصوص خاصة لمكافحة بعض مظاهر الإجرام المعلوماتي ؟ ما هي الجرائم التي يلزم مواجهتها بنصوص خاصة ؟ هل تغني هذه النصوص الخاصة عن النصوص العامة في حماية النظام المعلوماتي وفي الحماية من هذا النظام. ما هو الأثر الذي يخلفه وجود شبكة الإنترنت على جرائم الكمبيوتر ؟ ما السبيل إلى تقوية دور قانون العقوبات في مكافحة الجرائم التي تقع بطريق شبكة الأنترنت ؟

٩- خطة البحث:

يعالج هذا البحث موضوع دور قـانون العقوبـات ومكافحـة جـرائم الكمبيوتر من خلال الخطة التالية:

الفصل الأول: عدم كفاية النصوص العامة في قانون العقوبات لمكافحة جرائم الكمبيوتر.

الفصل الثاني: الحاجة إلى قواعد خاصة لمكافحة جرائم الكمبيوتر

الفصل الأول

عدم كفاية النصوص العامة في قانون العقوبات

لمكافحة جرائم الكمبيوتر

١٠- ترجع عدم كفاية النصوص العامة في قانون العقوبات لمكافحة جرائم الكمبيوتر إلى الطبيعة الخاصة للمعلومات والتي تميزها عن غيرها من الأموال المنقولة والعقارية . يضاف إلى ذلك اختلاف تدوين هذه المعلومات على أقراص ممغنطة أو على اسطوانات أو تخزينها في الجهاز نفسه ، الأمر الذي تختلف فيه عن المحررات التقليدية .

في هذا الفصل نوضح عدم كفاية النصوص العامة في حماية حق المؤلف وبراءة الاختراع لمكافحة جرائم الكمبيوتر **(في مبحث أول)** .

وعدم ملاءمة الأحكام العامة في جرائم الأموال لمكافحة جرائم الكمبيوتر **(في مبحث ثان)** .

ومدى اعتبار المعلومات المبرمجة محررات يحميها قانون العقوبات **(في مبحث ثالث)** .

المبحث الأول

عدم كفاية النصوص العامة في حماية حق المؤلف وبراءة الاختراع لمكافحة جرائم الكمبيوتر والإنترنت

١١- تكفل التشريعات المقارنة حماية محدودة للمعلومات المبرمجة داخل نظام الكمبيوتر من خلال قوانين حماية حق المؤلف وكذلك من خلال قوانين براءة الاختراع . كما أن ما تتضمنه بعض التشريعات من حماية جنائية لسر الصناعة يقتصر في مجاله على ما يشكل سرا للصنعة دون غيره من بيانات مبرمجة بالكمبيوتر(١) .

١٢- الحماية الجنائية للبرامج بمقتضى قانون حق المؤلف:

تحرص التشريعات المختلفة على حماية حق المؤلف من الناحية الجنائية، بالإضافة إلى الناحية المدنية وتسن من التشريعات ما يورد جزاءات جنائية عند الاعتداء على هذا الحق. وقد حرص المشرع المصري على توفير الحماية الجنائية لحق المؤلف بمقتضى القانون رقم ٣٥٤ لسنة ١٩٥٤ المعدل بالقانون رقم ٣٨ لسنة ١٩٩٢ . وقد تضمن هذا القانون نصا يمد حمايته فيه إلى برامج الحاسب الآلي. فتنص المادة الثانية منه على أن تشمل الحماية مصنفات الحاسب الآلي (٢). وبالمثل فإن القانون رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية في دولة الكويت تضمن في المادة الثانية منه بندا على

---

(١) انظر
Manfred Möhrenschlager , Computer Crimes and Other Crimes against Information Technology in Germany , Rev.int . dr. pén. 1993, p. 339 .

(٢) راجع لاحقا رقم ١٣ .

(مصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها) .
وأصبحت التشريعات المختلفة تتجه هذه الوجهة في التسوية بين المؤلفات وبين البرامج في الحماية الجنائية . وقد صرحت المادة الثانية / فقرة (ز) من القانون الاتحادي رقم ٤٠ لسنة ١٩٩٢ في شأن حماية المصنفات الفكرية وحقوق المؤلف بدولة الإمارات العربية المتحد على أن " وتشمل الحماية المصنفات الفكرية الآتية : .... ز) المصنفات السينمائية والتليفزيونية والإذاعية والأعمال الابتكارية السمعية والبصرية وبرامج الحاسوب ... " .
كما تتفق التشريعات الأمريكية والأوربية على أن برامج الكمبيوتر تتمتع بالحماية القانونية المقررة لحق المؤلف ، سواء في الجوانب المدنية لتلك الحماية أو في جوانبها الجنائية [١].

وقد أصدر المشرع الفرنسي قانونا خاصا في ٣ يوليو سنة ١٩٨٥ لتعديل القانون الصادر في ١١ مارس سنة ١٩٥٧ في شأن حماية الملكية الفكرية والفنية . وقد تضمن هذا التعديل حماية برامج الكمبيوتر باعتبارها من الأعمال الفكرية oeuvres de l'esprit [٢].

وقد اتجهت غالبية أحكام القضاء الفرنسي - قبل صدور هذ القانون - إلى اعتبار البرامج من قبيل أعمال الفكر oeuvre de l'esprit التي يحميها قانون حماية حق المؤلف[٣]. ويثور التساؤل عن مدى فعالية الحماية التي

---

(١) د. محمد حسام محمود لطفي ، المرجع السابق ص ١٥٥ .
(٢) انظر:
Jérôme Huet, Herbert Maisl, Droit de l'informatique et de télécommunications , Litec, 1989, p. 265
(٣) راجع
Trib Grande Inst. de Paris 10ème ch. , 9 mars 1982, Paris 4ème ch. A , 2 nov. 1982 , Trib Grand Instance de Paris 8 déc. 1982 ; Trib Grande Inst. de Paris, 3 ch. 27
juin 1984, I. R. droit de l'informatique. p. 39.

يوفرها قانون حماية حق المؤلف لبرامج وبيانات الحاسب الآلي وعن الحدود التي تقف عنده هذه القوانين عاجزة عن توفير تلك الحماية. ذلك ما سوف نحاول إيضاحه فيما يلي من عرض قانوني لتلك الأفكار .

١٣- النسخ بغرض البيع يشكل جريمة اعتداء على حق مؤلف البرامج :

يعتبر نسخ البرنامج لأغراض تجارية نوعا من التقليد الذي تتوافر به جريمة الاعتداء على حق المؤلف بطريق التقليد [١]. تشير القوانين الحديثة عادة إلى الحق في عمل نسخة واحدة للاستعمال الشخصي [٢] . وهذه الفكرة معمول بها في التشريعات الحديثة مثل القانون الإنجليزي [٣] والقانون الإسرائيلي [٤] ، حيث لا يترتب على النسخ للاستعمال الشخصي لبرامج الكمبيوتر سوى مسئولية مدنية إذا توافرت شروطها ، وليس مسئولية جنائية.

وقد تضمن القانون المصري هذا النص في المادة ١٢ من قانون حماية حق المؤلف على ما سبق بيانه . كما يشير إليه القانون رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية في الكويت في المادة (٨) منه بقوله " إذا قام شخص بعمل نسخة واحدة من مصنف وتمّ نشره أو قام بترجمته أو الاقتباس منه أو تصويره بأي شكل آخر وذلك لاستعماله الشخصي ، فلا يجوز

---

(١) د. على عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة الكترونيا ، مؤتمر جامعة الإمارات ، كلية الشريعة والقانون ، في الفترة ١- ٣ مايو سنة ٢٠٠٠ ص ٦ .

(٢) د. محمد حسام محمود لطفي ، المرجع العملي في الملكية الأدبية والفنية ، ١٩٩٥ ص ٥٣ .

(٣) انظر

Martin Wasik , Computer Crimes and Other Crimes against Information Technology in the United Kingdom , Rev.int. dr. pén. 1993, p. 632.

(٤) انظر :

Eli Lederman , Computer Crimes and Other Crimes against Information Technology in Israel , Rev.int.dr.pén. 1993,p.406.

للمؤلف أن يمنعه من ذلك . على أنه لا يجوز نشر هذه الأعمال إلاّ بإذن من صاحبها والمؤلف " .

وبناء عليه فإن من يقوم بنسخ برنامج للكمبيوتر يُسأل جنائيا ، كما يُسأل مدنيا ، ما دام أنه ينسخ بغرض البيع وليس للاستعمال الشخصي .

أما المشتري الذي يتفق معه البائع على عمل نسخة له ، فإنه يُسأل بوصفه شريكا في الجريمة ، وذلك بطريق الاتفاق ، ما دامت الجريمة – وهي النسخ – قد تمت بناء على ذلك الاتفاق .

أما في الفرض الذي يقوم فيه المشتري بشراء نسخة جاهزة ممن قام بنسخها في وقت سابق، فإن الجريمة لم تقع بناء على ذلك الاتفاق . ومع ذلك فإنه يسأل بوصفه مخفيا للأشياء المتحصلة من جريمة. فتنص المادة ٤٤ مكررا عقوبات على أنه " كل من أخفى أشياء مسروقة أو متحصلة من جناية أو جنحة مع علمه بذلك يعاقب بالحبس مع الشغل مدة لا تزيد على سنتين. وإذا كان الجاني يعلم أن الأشياء التي يخفيها متحصلة من جريمة عقوبتها أشد حُكم عليه بالعقوبة المقررة لهذه الجريمة ". ولا نرى أن هناك ما يحول دون اعتبار من يحصل على نسخة بدون وجه حق ويقوم باستعمالها مخفيا لشيء متحصل من الجريمة ، ذلك أن الإخفاء لا يقتصر على معناه المادي ، بل يشمل كل ما من شأنه أن يظهر الشيء وكأن المخفي يمارس عليه حقا قانونيا. ونرى أن ذلك متحقق في هذا الفرض.

ولا يصح التحدي في رأينا بأن المشتري إنما يقتني نسخة للاستعمال الشخصي، سواء قام هو بنفسه بالنسخ أو قام شخص أخر بالنسخ لحسابه ، وأن الأمر يتعلق بنسخة واحدة للاستعمال الشخصي. ذلك أن هناك فارقا بين أن يطلب المشتري إلى شخص آخر بعمل نسخة شخصية له وأن يقوم

بشراء نسخة جاهزة من ذلك الذي يبيع عددا من النسخ. في الفرض الأول يتعلق الأمر بعمل نسخة شخصية وبالتالي لا جريمة من الناسخ لأنه يعمل لحساب المشتري. ولا جريمة من المشتري لأنه يطلب نسخة للاستعمال الشخصي . أما في الفرض الثاني فإن الأمر يتعلق بشراء من شخص يرتكب جريمة الاعتداء على حق المؤلف. ومن هنا كان الفارق بين الفرضين من الوجهة القانونية.

ويلاحظ أن القانون الكويتي يجعل من يقوم بإخفاء الأشياء المتحصلة من ارتكاب الجريمة أو التي استعملت في ارتكابها شريكا في الجريمة (مادة ٤٩ من قانون الجزاء) . وليس ثمة فارق آخر بين القانون الكويتي والقانون المصري في مدى مسئولية المشتري على النحو الذي سبق أن أوردناه .

١٤- حدود الحماية الجنائية لحق المؤلف في مجال البرامج والمعلومات:

يبين من مراجعة قانون حق المؤلف أنه يمكن أن يقوم بدور في حماية برامج الكمبيوتر . لكن هناك من القيود ما يحدّ من هذا الدور وبالتالي من فعالية هذا النوع من القوانين في توفير الحماية الجنائية الكاملة للمعلومات المبرمجة آليا (التي يحتويها جهاز الكمبيوتر).

وتظهر تلك الحدود من الآتي:

١-إن قانون حماية حق المؤلف لا يحمي المعلومات التي يحتويها جهاز الكمبيوتر. فهو لا يحمي إلاّ البرامج .

ومؤدى ذلك أن المعلومات التي تقوم الإدارات العامة والشركات وكذلك يقوم الأفراد بتخزينها ومعالجتها في أجهزة الكمبيوتر الخاصة بهم لا تتمتع بالحماية التي يوفرها قانون حماية حق المؤلف. ومن هنا كان قصور هذا

النوع من القوانين عن تحقيق الحماية الجنائية الكاملة للبيانات المعالجة آليا (الموجودة بالكمبيوتر) .

٢- إن الحماية التي يوفرها قانون حماية حق المؤلف لبرامج الحاسب الآلي لا تتحقق لجميع البرامج . فمن المتعين توافر عدة شروط ، أهمها شرط الابتكار[١].

وقد عبر قانون حماية حق المؤلف في مصر رقم ٣٥٤ لسنة ١٩٥٤ عن ذلك الشرط في المادة الأولى منه بقوله "يتمتع بحماية هذا القانون مؤلفو المصنفات المبتكرة في الآداب والفنون والعلوم أيا كان نوع هذه المصنفات أو طريقة التعبير عنها وأهميتها أو الغرض من تصنيفها . ... " . وفي نفس الاتجاه تنص المادة الأولى من القانون الكويتي رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية على أنه "يتمتع بحماية هذا القانون مؤلفو المصنفات المبتكرة في الآداب والفنون والعلوم أيا كانت قيمة هذه المصنفات أو نوعها والغرض من تأليفها أو طريقة التعبير عنها .... " .

٣- لا يحمي قانون حماية حق المؤلف من البرامج إلاّ ما صدر بها قرار من وزير الثقافة . فتنص المادة الثانية من القانون رقم ٣٥٤ لسنة ١٩٥٤ في شأن حماية حق المؤلف في مصر بعد تعديله بالقانون رقم ٣٨ لسنة ١٩٩٢ على أن تشمل الحماية المنصوص عليها في هذا القانون مؤلفي : ... - مصنفات الحاسب الآلي من برامج وقواعد وبيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة " . ويختلف الوضع في القانون الكويتي حيث

---

(١) د. محمد حسام محمود لطفي ، المرجع العملي في الملكية الأدبية والفنية " ١٩٩٥ ص ٤٢٦؛ انظر للمؤلف نفسه : الحماية القانونية لبرامج الحاسب الإلكتروني ، دار الثقافة ١٩٨٧ ص ١٠٣ .

أشارت المادة الثانية من القانون رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية إلى مصنفات الحاسب الآلي ولم تشترط أن يصدر قرار وزاري بتحديد تلك البرامج محل الحماية .

٤- إن قانون حماية حق المؤلف لا يحول دون أن يقوم شخص الغير بعمل نسخة للاستعمال الشخصي. فتنص المادة ١٢ من قانون حماية حق المؤلف بعد تعديله على أن "لا يجوز للمؤلف الذي نشر مصنفه بإحدى الطرق المبينة بالمادة (٦) من هذا القانون أن يمنع أي شخص من عمل نسخة وحيدة من هذا المصنف لاستعماله الشخصي ، وكذلك المصنفات السمعية والسمعية البصرية إذا تم إذاعتها كاملة بالإذاعة أو عرضها بالتليفزيون " .

ولا شك أن أحكام المسئولية المدنية تأتي عونا لسد النقص في أحكام المسئولية الجنائية في حالات كثيرة [١] . من تلك الحالات ما يتعلق ببرامج الكمبيوتر ، حيث يكون للمشتري أن يضمن شرطا بالحفاظ على سرية البرامج في عقد الشراء الذي محله تلك البرامج [٢] .

وقد دعت سهولة نسخ برامج الكمبيوتر الشركات التي تقوم ببيع اسطوانات البرامج إلى وضع شروط للبيع ملحقة بتلك الاسطوانات . وتفترض تلك الشركات أن المشتري قد قبل عند شرائه بأن يفي بالالتزامات الملحقة باسطوانة البرامج . وكثيرا ما يتضمن العقد شرطا يحظر على المشتري

---

(١) د. نزيه محمد الصادق المهدي ، الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية ، مؤتمر " القانون والكمبيوتر والإنترنت " جامعة الإمارات ، كلية الشريعة والقانون ، ١- ٣ مايو سنة ٢٠٠٠ ، المجلد الأول ص ٢ .

(٢) د. محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسب الإلكتروني ، أبحاث مؤتمر الكويت للقانون والحاسب الالي ، منشورات جامعة الكويت ومؤسسة التقدم العلمي ١٩٩٤ ص ٢٥ .

أن يقوم بنسخ اسطوانة البرنامج محل البيع ولو كان لنسخة واحدة . من أجل ذلك تدخل المشرع المصري بنص المادة (١٢) من قانون حماية حق المؤلف ليمنع مثل هذا الشرط بقوله "لا يجوز للمؤلف الذي نشر مصنفه بإحدى الطرق المبينة بالمادة (٦) من هذا القانون أن يمنع أي شخص من عمل نسخة وحيدة من هذا المصنع لاستعماله الشخصي ، وكذلك المصنفات السمعية والسمعية البصرية إذا تمت إذاعتها كاملة بالإذاعة أو عرضها بالتليفزيون " .

١٥- الحماية الجنائية لبراءة الاختراع :

تحرص التشريعات المختلفة على توفير حماية جنائية لبراءة الاختراع ، بالإضافة إلى توفير الحماية المدنية . ويعالج القانون رقم ١٣٢ الصادر في ١٦ أغسطس سنة ١٩٤٩ والمعدل بالقانون رقم ٦٥٠ لسنة ١٩٥٥ والخاص ببراءة الاختراع والرسوم والنماذج الصناعية هذا الموضوع .

وتحدد المادة الأولى من القانون السابق الشروط التي تمنح بمقتضاها براءة الاختراع . فتنص هذه المادة على أن " تُمنح براءة الاختراع وفقا لأحكام هذا القانون عن كل ابتكار جديد قابل للاستغلال الصناعي سواء أكان متعلقا بمنتجات صناعية جديدة أم بطرق أو وسائل صناعية مستحدثة أم بتطبيق جديد لطرق أو وسائل صناعية معروفة " .

ولا تخرج التشريعات المقارنة عن نفس الفكرة . فينص القانون رقم ٤ لسنة ١٩٦٢ في الكويت في شأن براءات الاختراع والرسوم والنماذج الصناعية في مادته الأولى على أن " تمنح براءات اختراع وفقا لأحكام هذا القانون عن كل ابتكار جديد قابل للاستغلال الصناعي سواء أكان متعلقا بمنتجات صناعية جديدة أم بطرق أو وسائل صناعية مستحدثة أم بتطبيق

جديد لطرق أو وسائل صناعية معروفة".

وتقرر المادة ٤٨ من القانون ذاته عقوبة للتقليد والبيع والعرض للبيع والاستيراد والحيازة لمنتجات مقلدة لبراءة اختراع مسجلة في مصر[(١)]. فتنص تلك المادة على أن " يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن عشرة جنيهات ولا تزيد على ثلاثمائة جنيه أو بإحدى هاتين العقوبتين :

(١) كل من قلد موضوع اختراع مُنحت عنه براءة وفقا لهذا القانون .

(٢) كل من قلد موضوع رسم أو نموذج صناعي تم تسجيله وفقا لهذا القانون.

(٣) كل من باع أو عرض للبيع أو للتداول أو استورد من الخارج أو حاز بقصد الاتجار منتجات مقلدة أو مواد عليها رسم أو نموذج صناعي مقلد مع علمه بذلك متى كان الاختراع أو الرسم أو النموذج مسجلا في مصر .

(٤) كل من وضع بغير حق على المنتجات أو الإعلانات أو العلامات التجارية أو أدوات التعبئة أو غير ذلك براءة اختراع أو بتسجيله رسما أو نموذجا صناعيا " .

وقد نصت المادة ٤٦ من هذا القانون الكويتي رقم (٤) لسنة ١٩٦٢ في شأن براءات الاختراع والرسوم والنماذج الصناعية على صور للتجريم التي لا تخرج عما سبق أن أورده القانون المصري . فالتقليد والبيع والعرض للبيع والاستيراد والحيازة بقصد الاتجار لمنتجات مقلدة وكذلك وضع علامة على

---

(١) د. سينوت حلم دوس ، تشريعات براءات الاختراع ، منشأة المعارف ، الإسكندرية ١٩٨٨ ص٣٠.

المنتجات تدل على الحصول على براءة اختراع ، كلها صور تعاقب عليها بعقوبة الحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن عشرة دنانير ولا تزيد على مائتين وخمسة وعشرين دينارا أو بإحدى هاتين العقوبتين .

وتتضمن تشريعات خليجية أخرى أحكاما متشابهة . فينص القانون الاتحادي لدولة الإمارات العربية المتحدة رقم ٤٤ لسنة ١٩٩٢ في شأن تنظيم وحماية الملكية الصناعية لبراءات الاختراع والرسوم والنماذج الصناعية على الحماية المدنية والجنائية لبراءات الاختراع . فتنص المادة ٦٠ من القانون السابق على عقوبة الحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين والغرامة التي لا تقل عن خمسة آلاف درهم أو إحدى هاتين العقوبتين لتقليد الاختراع المسجل أو طريقة صنعه أو عنصرا من عناصر الدراية العملية أو الاعتداء عمدا على أي حق يحميه قانون براءات الاختراع.

وقد أضاف القانون رقم ٢٣ لسنة ١٩٥١ معدلا بالقانون رقم ٣٨ لسنة ١٩٦١ بمزاولة مهنة وكلاء البراءات في مصر عقوبة لمن يدعي على خلاف الحقيقة بأنه وكيل براءات . فتنص المادة السابقة على أنه "مع عدم الإخلال بعقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تجاوز مائتي جنيه أو بإحدى هاتين العقوبتين كل شخص اسمه غير مقيد في السجل يستعمل نشرات أو لافتات أو أية وسيلة أخرى من وسائل الدعاية إذا كان من شأن ذلك أن يحمل الجمهور على الاعتقاد بأن له الحق في مزاولة مهنة وكيل براءات وكذلك كل شخص ينتحل لنفسه هذه الصفة . وفي جميع الأحوال يأمر القاضي بنزع اللوحات واللافتات ونشر الحكم في صحيفتين يعينهما على نفقة المحكوم عليه" .

١٦ - عدم ملاءمة قانون براءة الاختراع لحماية برامج الكمبيوتر:

تظهر عدم الملاءمة من الآتي :

١ - لا يتحقق لبرامج الكمبيوتر شروط براءة الاختراع : ومن أهمها شرط القابلية للاستغلال الصناعي الذي تتطلبه المادة الأولى من براءة الاختراع سابق الإشارة إليه [١].

٢ - لا يحمي قانون براءة الاختراع المعلومات العادية التي تحتفظ بها الإدارات الحكومية والشركات الخاصة وكذلك الأفراد في أجهزتهم . فهذه البيانات لا يمتد إليها وصف الاختراع بحال من الأحوال .

٣ - تقتصر الحماية المقررة في قانون براءة الاختراع على صور معينة من النشاط . هذه الصور هي التقليد والبيع والعرض للبيع والاستيراد والحيازة . أما اختلاس المعلومات وتغيير البيانات المعالجة آليا (الموجودة بالجهاز) والاعتداء على حرمة الحياة الخاصة ، فإن قانون براءة الاختراع لا يمتد إليها .

ومع ذلك فإن برامج الحاسب الآلي يمكن أن تستفيد من الحماية الجنائية المقررة لبراءة الاختراع إذا كانت الوسيلة الصناعية التي تم اختراعها تعتمد في مرحلة من مراحلها على عمل برنامج من برامج الحاسب الآلي . وقد قضت بذلك المحاكم الفرنسية في أحكام لها [٢].

---

(١) د. جلال أحمد خليل ، النظام القانوني لحماية الاختراعات ونقل التكنولوجيا إلى الدول النامية ، مطبوعات جامعة الكويت ، مجلس النشر العلمي ، ١٩٨٣ ، ص ١٠٦ .

(٢) د. سينوت حليم دوس ، تشريعات براءات الاختراع ، منشأة المعارف ، الإسكندرية ١٩٨٨ ص٣٠ .

١٧ - حماية البرامج بمقتضى قانون العلامة التجارية :

تحرص كثير من القوانين على توفير الحماية الجنائية للعلامة التجارية ، بالإضافة إلى الحماية المدنية [١]. وعادة ما توجد في قوانين خاصة لحماية العلامات التجارية من التقليد. وقد أفرد المشرع المصري القانون رقم ٥٧ لسنة ١٩٣٩ المعدل للحماية المدنية والجنائية للعلامات التجارية . وتُعرف العلامة التجارية بأنها " هي التي يتخذها الصانع أو التاجر شعارا لمنتجاته أو بضائعه أو خدماته تمييزا لها عن غيرها من المنتجات والبضائع والخدمات المباعة " [٢] .

في ذلك تنص المادة ٣٣ من قانون العلامات التجارية في مصر على أنه يُعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسين جنيها ولا تزيد على ٣٠٠ جنيها أو بإحدى هاتين العقوبتين : ١- كل من زور علامة تم تسجيلها طبقا للقانون أو قلدها بطريقة تدعو إلى تضليل الجمهور وكل من استعمل بسوء القصد علامة مزورة أو مقلدة . ٢- كل من وضع بسوء القصد على منتجاته علامة مملوكة للغير. ٣- كل من باع أو عرض للبيع أو للتداول أو حاز بقصد البيع منتجات عليها علامة مزورة أو مقلدة أو موضوعة بغير حق مع علمه بذلك .

وقد اهتمت بعض التشريعات الخليجية بإفراد نصوص خاصة لحماية العلامة التجارية[٣]. من ذلك أن قانون التجارة الكويتي قد أورد أحكاما جنائية لحماية العلامة التجارية . فتنص المادة ٩٢ من ذلك القانون على أن

---

(١) د. فايز عبد الله الكندري ، الحماية المدنية لبرامج الحاسب الآلي في القانون الكويتي ، في أعمال مؤتمر " القانون والكمبيوتر والإنترنت " نظمته جامعة الإمارات ، كلية الشريعة والقانون ، في الفترة من ١-٣ سنة ٢٠٠٠ ، ص ٥ .

(٢) د. مصطفى كمال طه " القانون التجاري ، دار الجامعة الجديدة للنشر ، ١٩٩٠ ص ٥٩٩

(٣) د. يعقوب يوسف صرخوه ، النظام القانوني للعلامات التجارية ، دراسة مقارنة ، جامعة الكويت ، مجلس النشر العلمي ، ١٩٩٢ - ١٩٩٣ ، ص ١٨٩ .

"يُعاقب بالحبس وبغرامة لا تزيد على ستمائة دينار أو بإحدى هاتين العقوبتين : ١ - كل من زور علامة تم تسجيلها طبقا للقانون أو قلدها بطريقة تدعو إلى تضليل الجمهور ، وكل من استعمل وهو سيئ النية على منتجاته علامة مملوكة للغير . ٣ - كل من باع أو عرض للبيع أو للتداول (أو حاز بقصد البيع منتجات عليها علامة مزورة أو مقلدة أو موضوعة بغير حق مع علمه بذلك . ٤ - كل من خالف وهو سيئ النية أحكام المواد ٨٧ - ٩١ الخاصة بالبيانات التجارية " . وبالمثل فإن القانون الاتحادي رقم ٣٧ لسنة ١٩٩٢ في شأن العلامات التجارية في دولة الإمارات العربية المتحدة . فتنص المادة ٣٧ منه على عقوبة الحبس والغرامة التي لا تقل عن ٥٠٠ درهم أو إحدى هاتين العقوبتين لكل من : ١- زور العلامة التجارية . ٢- استعمل بغير حق علامة تجارية لغيره . ٣ - وضع بسوء نية علامة تجارية مسجلة للغير على منتجاته . ٤ - بيع أو عرض للبيع علامة تجارية مقلدة . ٥ - عرض تقديم خدمات تحت علامة تجارية مقلدة .

هذه الأحكام تنسحب في حمايتها على برامج الحاسب الآلي التي وضع لها صانعها أو المتاجر فيها علامة تجارية وقام الغير بتقليد تلك العلامة مع نسخ البرنامج لبيعه .

ومع ذلك فإن تلك الحماية الجنائية المقررة للعلامة التجارية لا تكفي لحماية برامج وبيانات الكمبيوتر ، وذلك للأسباب التالية :

- إن هذه الأحكام لا تحمي إلاّ البرامج التي لها علامة تجارية . صحيح أن الغالبية من تلك البرامج لها علامة تجارية ، إلاّ أنه من المتصور وجود البعض منها الذي ليس له علامة تجارية . هذا النوع من البرامج يبقى خارج مجال تلك الحماية .
- لا تحمى أحكام العلامات التجارية البيانات المبرمجة في الكمبيوتر ، إذ لا علاقة لها بالعلامات التجارية .

- لا تحمي أحكام العلامة التجارية البرامج إذا قام الغير بتقليد هذا البرنامج دون تقليد العلامة التجارية . ويكشف هذا بوضوح عن أن قانون العلامات التجارية أُعد خصيصا لحماية العلامة التجارية وليس لحماية برامج الكمبيوتر. ولا عجب في ذلك ، إذ إن قوانين العلامات التجارية قد شُرعت قبل تداول برامج الكمبيوتر . فقانون العلامات التجارية في مصر يرجع إلى سنة ١٩٣٩ وإن كان محلا لتعديلات لاحقة .

١٨- تكامل الحماية المدنية والحماية الجنائية لبرامج الكمبيوتر :

تبدو أوجه القصور في قانون حماية حق المؤلف عند تطبيقه على المعلومات وبرامج الكمبيوتر عائدة إلى الطبيعة الخاصة لهذه الأموال محل الحماية، وإلى أن قانون حماية حق المؤلف إنما صُمم أساسا لحماية الكتب والمراجع العلمية وليس بيانات الكمبيوتر .

غير أن هذه الحماية المدنية تثير بعض المشكلات القانونية حول مدى توافر رضاء المشتري بالعقد الذي أرفقه البائع بلفافة الاسطوانة والتي قد لا يدري عنها المشتري شيئا إلاّ بعد إتمام عملية الشراء : هل ثمة عقد بين المشتري وبين البائع ؟ ما هو الدليل على موافقة المشتري على ذلك العقد في غياب ما يدل على توقيع المشتري على وثيقة العقد ؟ كما يُثار التساؤل عن طبيعة هذا العقد إن وجد : هل هو عقد إذعان أم لا ؟ وهل من حق البائع أن يفرض مثل هذا النوع من العقود إذا كان عقد إذعان ؟

وعلى العموم فإنه حتى ولو لم تُطبق أحكام المسئولية التعاقدية على الإخلال بالشروط الخاصة بشراء برامج الكمبيوتر ، فإن أحكام المسئولية التقصيرية ومنها ما يتصل بالمنافسة غير المشروعة سوف تجد محلا لها لكي تحمي صاحب الحق في تلك البرامج [1].

---

(١) د. أحمد ضاعن السمدان ، الحماية القانونية المدنية لبرامج الكمبيوتر وصورها وتطبيقاتها في القانون المقارن وفي دول الخليج ، أعمال مؤتمر جامعة الكويت حول " القانون والحاسب الآلي " مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي ، ١٩٩٤ ص ٥٩ .

المبحث الثاني

عدم ملاءمة الأحكام العامة في جرائم الأموال

لمكافحة جرائم الكمبيوتر

١٩- يقصد بالأحكام العامة في جرائم الأموال تلك التي تعاقب على السرقة والنصب وخيانة الأمانة . هذه النصوص وضعت لحماية الأموال . ويقصد بالأموال هنا الأموال المنقولة ، ذلك أن الأموال العقارية لها نصوص مستقلة تحميها. يضاف إلى ذلك ما قدره المشرع من ضعف الأموال المنقولة، الأمر الذي يستوجب حمايتها من العدوان عليها في شكل سرقة أو نصب أو خيانة أمانة.

وقد ظهر قصور هذه النصوص عن حماية المعلومات بسبب الطبيعة الخاصة التي تتميز بها والتي أثارت الشك حول اعتبارها من المنقولات أو من الأفكار . وهذا ما نعالجه في (المطلب الأول) من هذا المبحث.

يضاف إلى ذلك اختلاف مفهوم الاختلاس في السرقة عن هذا المفهوم إذا تعلق الأمر بالمعلومات. فالعدوان على ملكية وعلى حيازة المعلومات يتخذ مفهوما مختلفا عنه إذا وقع على ملكية وحيازة المنقولات . وهذا ما نعالجه في (المطلب الثاني) من هذا المبحث .

المطلب الأول

الصعوبات القانونية المتعلقة بتطبيق أحكام السرقة على جرائم الكمبيوتر

٢٠ - نظرا للطبيعة الخاصة للمعلومات المعالجة بالكمبيوتر، ونظرا لحداثة ظهور هذا النوع من الأموال، ونظرا لأن القواعد التقليدية في العقاب على السرقة قد وضعت في وقت سابق على ظهور الكمبيوتر ، فإن صعوبات قانونية تتعلق بإعمال القواعد المقررة في السرقة قد ظهرت في أحكام القضاء وآراء الفقه.

من هذه الصعوبات ما يتعلق بمدى اعتبار المعلومات مالا منقولا (الفرع الأول) .

ومنها ما يتعلق بمفهوم الاختلاس (الفرع الثاني).

وأخيرا منها ما يتعلق بتوافر القصد الجنائي وخاصة نية التملك (الفرع الثالث) .

الفرع الأول

مدى اعتبار المعلومات مالا منقولا

في مفهوم جريمة السرقة

٢١- جرائم الأموال تحمي المنقول دون غيره :

خصّ المشرع في البلدان المختلفة المنقول بعناية خاصة ، نظرا لما يتميز به من ضعف يتمثل في قابليته للانتقال وبالنظر إلى حكم الظاهر الذي رتب عليه القانون أن الحيازة في المنقول سند الملكية . هذا الأمر يختلف إذا تعلق الأمر بالعقارات.

فتنص المادة ٣١١ من قانون العقوبات في مصر على أن " كل من اختلس منقولا مملوكا لغيره فهو سارق" . كما يبين من المادة ٣٣٦ عقوبات مصري أن المال محل الحماية في جريمة النصب هو المنقول ، فتنص هذه المادة على أن " يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو مخالصة أو أي متاع منقول .... " . وبالمثل فإن المنقول هو المقصود بالحماية في جريمة خيانة الأمانة ، فتنص المادة ٣٤١ عقوبات مصري على أن "كل من اختلس أو استعمل أو بدد مبالغ أو أمتعة أو بضائع أو نقودا أو تذاكر أو كتابات أخرى مشتملة على تمسك أو مخالصة أو غير ذلك ...... " .

ولم يخرج قانون الجزاء الكويتي عن هذا المفهوم على الرغم من عمومية صياغة المادة ٢٤٠ منه والتي أشارت إلى المال المملوك للغير دون أن تشترط صراحة أن يكون مالا منقولا . فتنص المادة السابقة على أن " كل من حاز مالا مملوكا لغيره بناء على وديعة أو عارية أو إيجار أو رهن أو وكالة أو عقد

آخر يلزمه بالمحافظة على المال وبرده عينا أو باستعماله في أمر معين لمصلحة مالكه أو أي شخص آخر وتقديم حساب عن هذا الاستعمال . ... " .

وقد وردت نصوص قانون العقوبات الاتحادي في دولة الإمارات العربية المتحدة في نفس الاتجاه . فتنص المادة (٣٨٣) على أن "تقع السرقة التعزيرية باختلاس مال منقول مملوك لغير الجاني ... " . كما تقع جريمة النصب وفقا لقانون العقوبات الاتحادي بدولة الإمارات على منقول . فتنص المادة (٣٩٩) منه على أن "يعاقب بالحبس أو بالغرامة كل من توصل إلى الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع هذا السند أو إلى إلغائه أو إتلافه أو تعديله ، وذلك بالاستعانة بطريقة احتيالية ...." . وفي نفس الاتجاه تنص المادة ٤٠٤ عقوبات اتحادي على أن "يعاقب بالحبس أو بالغرامة كل من اختلس أو استعمل أو بدد مبالغ أو سندات أو أي مال آخر منقول إضرارا بأصحاب الحق عليه متى كان قد سلم إليه على وجه الوديعة أو الإجارة أو الرهن أو عارية الاستعمال أو الوكالة .... " .

أما في القانون الفرنسي ، فقد عُني المشرع – في قانون العقوبات المعمول به ابتداء من سنة ١٩٩٤ – بعدم استعمال تعبير " مال منقول مملوك للغير " كمحل لجرائم السرقة والنصب وخيانة الأمانة . فتنص المادة ٣١١/ ١ عقوبات فرنسي على أن " السرقة هي اختلاس شيء مملوك للغير بنية الغش "[1] . كما عبرت المادة ٣١٤ – ١ عقوبات عن محل جريمة خيانة الأمانة بأنه " مال أيا كان "[2] . وقد وسّعت المادة ٣١٣ / ١ عقوبات

---

1)) " Le vol est la soustraction frauduleuse de la chose d'autrui " (art. 311-1) .

2)) " L'abus de confiance est le fait par une personne de détourner , au préjudice d'autrui des fonds , des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre , de les représenter ou d'en faire un usage déterminé. " (art. 314 – 1) .

فرنسي – بعد التعديل الذي أصبح ساريا في سنة ١٩٩٤ – من مجال جريمة النصب بحيث تسري على الخدمات وليس على المال المنقول المملوك للغير فقد ، كما كانت تقضي بذلك القواعد العامة والتي لا يزال يعتنقها قانون العقوبات المصري [(١)] .

٢٢- صعوبة اعتبار المعلومات منقولات :

واجهت المحاكم عدة صعوبات قانونية في اعتبار المعلومات من قبيل المنقولات. وقد ترتب على ذلك أن استبعد القضاء في دول مختلفة تطبيق وصف السرقة عندما يتعلق الأمر بالمعلومات المبرمجة [(٢)] . من ذلك أن المحكمة العليا في كندا قد قضت بأن المعلومات ليست من المنقولات في مفهوم القانون الجنائي [(٣)] .

وترجع معظم هذه الصعوبات إلى الآتي :

١- المعلومات ليست من الأشياء :

الأصل أن صفة المنقول لا تثبت إلاّ للأشياء. هذه الأشياء تختلف عن الأفكار [(٤)] .

---

(1) " L'escroquerie est le fait , soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité, soit par l'emploi de manoeuvres frauduleuses , de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers , à remettre des fonds , des valeurs ou un bien quelconque , à fournir un service ou à consentir un acte opérant obligation ou déchgarge " .
L'escroquerie est punie de cinq ans d'emprisonnement et de 500 000 F d'amende " (art. 313- 1) .

(٢) مثال ذلك المحاكم الكندية . انظر
: K . Piragoff , Computer Crimes and Other Crimes against Information Technology in Canada , in " Délits informatiques et autres infractions à la technologie de l'information " , Rev. dr. pén. 1993, p. 206.

(٣) انظر
Regina v. Stewart , (1988) 1 S.C.R.963 .

(٤) د. هشام محمد فريد رستم ، " قانون العقوبات ومخاطر تقنية المعلومات " مكتبة الآلات الحديثة ١٩٩٢ ص ٢٩ .

فالقانون المدني المصري يعرف المنقول بأنه ما يمكن فصلة ونقله دون تلف. في ذلك تنص المادة ٨٢ من القانون المدني المصري على أن "كل شيء مستقر بحيزه ثابت فيه لا يمكن نقله منه دون تلف ، فهو عقار وكل ما عدا ذلك من شيء فهو منقول" . وتنص المادة ٨٣ مدني مصري على أن "يعتبر مالا عقاريا كل حق عيني يقع على عقار ، بما في ذلك حق الملكية ، وكذلك كل دعوى تتعلق بحق عيني على عقار. (٢) ويعتبر مالا منقولا ما عدا ذلك من الحقوق المالية. وقد عرّفت المادة ٢٧ من القانون المدني الكويتي المنقول بقولها " يُعتبر عقارا كل حق عيني يقع على عقار " . وقد سبق أن عرّفت المادة ٢٤ مدني العقار بقولها " كل شيء مستقر بحيزه ، ثابت فيه لا يمكن نقله منه دون تلف أو تغيير في هيئته فهو عقار ... " .

يبين من ذلك كله أن المنقول لا يكون إلاّ شيئا. فهذه الصفة لا تثبت للأفكار[1] . هذه الأفكار يمكن أن ترد عليها حقوق مالية كحق المؤلف ولكن لا يرد عليها حقوق عينية كما هو الحال في الأشياء المنقولة والأشياء العقارية. من هذه الحقوق العينية حق الملكية. كما أن الحيازة لا ترد إلاّ على الأشياء المحسوسة، ولا يتصور أن ترد على الأفكار.

استنادا إلى نفس الفكرة أيضا قيل بعدم وقوع جريمة الإتلاف بالمادة ٣١١ من قانون العقوبات، مادامت هذه المادة تنص على عقاب "كل من خرّب أو أتلف عمدا أموالا ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة ... "[2].

ويلاحظ أن كثيرا من الجرائم التي تقع بطريق الكمبيوتر تتمثل في

---

(١) د. هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية ١٩٩٢ ص ٥١ .

(٢) د. جميل عبد الباقي الصغير ، " القانون الجنائي والتكنولوجيا الحديثة " ، دار النهضة العربية ١٩٩٢ ص ١٥٧.

إجراء تحويلات نقدية وذلك بإعطاء أمر بطريق الغش إلى أجهزة الكمبيوتر الخاصة بأحد البنوك أو المصارف. لا تعتبر بعض التشريعات تلك التحويلات واردة على مال منقول مملوك للغير، بل تعتبرها منشئة حقا للبنك المحول إليه في ذمة البنك المحول منه[1]. وبناء عليه لا تعتبر تلك التشريعات أن إجراء تلك التحويلات بطريق الغش مشكل لجريمة سرقة أو نصب . من تلك التشريعات التشريع البلجيكي والألماني واليوناني والياباني والقانون في لكسمبورج [2] .

بل إن هذه التشريعات سابقة الذكر (قانون العقوبات البلجيكي وقانون العقوبات الإيطالي وقانون العقوبات لدولة لكسمبورج)[3] تستلزم لوقوع جريمة السرقة أن يرد الاختلاس على شيء محسوس tangible property مع نية حرمان المجني عليه نهائيا من هذا المنقول with the intention of permanently depriving the victim .

بيد أن معظم التشريعات المقارنة تعتبر ذلك مشكلا لتسليم رمزي تقع به جريمة من جرائم الأموال كالسرقة والنصب وخيانة الأمانة وفقا للوصف القانوني الصحيح. من تلك التشريعات القانون الكندي الهولندي والسويسري والقانون الإنجليزي ومعظم قوانين الولايات في الولايات المتحدة الأمريكية[4] .

---

(1) a claim

(٢) انظر:

Ultrich Sieber, The international Handbook on Computer Crime, John Wiley & Sons, New York , 1986, p. .٣٩

(٣) انظر الفصل ٤٦١ من قانون العقوبات البلجيكي والفصل ٦٢٤ من قانون العقوبات الإيطالي) .

(٤) انظر

Ultrich Sirber, id, at 39 .

٢- المعلومات لا ترد عليها الحيازة:

من المعروف أن جرائم السرقة تقع عدوانا على الحيازة ، كما تقع على الملكية. و يصعب تصور حيازة المعلومة لأن لها كيانا معنويا، إذ الحيازة لا تتصور إلا بالنسبة للأشياء التي يرد عليها الاتصال المادي.

٣- المعلومات لا تبرح مكانها بالنسخ:

تتميز المعلومات عن المنقولات بأنها تبقى مدونة على الدعامة التي تحملها على الرغم من نسخها على شريط أو اسطوانة. وفي ذلك تختلف المعلومات عن غيرها من المنقولات التي لا تبقى بعد تحريكها.

ومع ذلك فقد استشعرت أحكام القضاء ضرورة حماية حق صاحب هذه المعلومات في ملكيتها، بالإضافة إلى حيازتها. وقد استتبع ذلك إعادة النظر في الطبيعة القانونية للمعلومات والبدء في الاعتراف لها بصفة الأموال. ومن هنا بدأ التعارض في توفير الحماية القانونية لها بوصفها من الأفكار وإضفاء صفة الأموال عليها لكي تنسحب الحماية القانونية المقررة للأموال

٢٣- الأساس القانوني لاعتبار المعلومات من المنقولات:

انطلاقا من الحاجة إلى حماية المعلومات المبرمجة من العدوان عليها في شكل سرقة أو نصب أو خيانة أمانة ، اتجهت أحكام القضاء في كثير من الدول إلى اعتبار المعلومات من المنقولات إذا كانت مسجلة على دعامة مادية . وقد حدث ذلك قبل أن يتدخل المشرع في هذه الدول بنصوص صريحة لتضفي عليها نفس الحماية الجنائية ولكن بنصوص خاصة .

غير أنه يتعين بادئ ذي بدء التمييز بين عدة أوضاع :

الوضع الأول :

وفيه يقوم المتهم بالاستيلاء على شريط أو اسطوانة . في هذه الحالة يتعلق الأمر بمال منقول ، حيث إن الشريط أو الاسطوانة المدون عليها معلومات تشكل ولا ريب مالا منقولا . مثلهما في ذلك مثل المستندات التي

يحميها تجريم السرقة والنصب وخيانة الأمانة . ولا يعتبر القول بذلك نوعا من الاجتهاد القضائي.

الوضع الثاني :

وفيه يقوم المتهم بنسخ المعلومات المبرمجة. سواء في الجهاز نفسه أو على اسطوانة أو شريط ، تاركا المعلومات الأصلية بالجهاز أو بالاسطوانة أو الشريط الأصلي .

في هذا الوضع الثاني لا يكون المتهم قد استولى على مال مادي منقول ينتمي إلى صاحبة ، بل يكون قد استولى على المعلومات ، وخاصة إذا قام بإحضار الشريط أو الاسطوانة من ماله الخاص . وهنا كانت محاولة القضاء اعتبار توفير الحماية القانونية للمعلومات على الرغم من أنها من الأموال ذات الطابع المعنوي . فاتجهت هذه الأحكام إلى القول بوقوع السرقة، مادام أن هذه المعلومات مسجلة على دعامة مادية . وسوف نبين الحجة التي استند إليها القضاء للوصول إلى ما انتهى إليه.

الوضع الثالث :

وفيه يقوم المتهم بالاطلاع على المعلومات دون نسخها. في هذه الحالة ترفض أحكام القضاء القول بأن المتهم قد استولى على منقولات . من ذلك ما قضي به من أنه وإن جاز القول بوقوع السرقة على مستند معين يتضمن شروط العقد ، فإن السرقة لا تقع على أحد بنود هذا العقد . ذلك أن هذا البند يشكل المحتوى القانوني للمستند[1]. وهنا نعود إلى حقيقة الأمر في تحديد المعلومات ؛ فهي لا تعدو أن تكون من الأفكار. فالاطلاع هنا هو

---

(1) Crim. 9 mars 1987, J.C,P. 1988, II, 2093

اطلاع على مجرد أفكار. ومن هنا يبدو التناقض بين اعتبار المعلومات منتمية تارة إلى المنقولات وتارة أخرى إلى الأفكار.

وهذا الحل هو المعمول به في قوانين عديدة حيث قُضي في إنجلترا في قضية Oxford v. Moss بعدم وقوع جريمة السرقة من الطالب الذي توصل بطريق الغش إلى الاطلاع على أوراق أسئلة الامتحان دون أن يستولي عليها [١] .

وعدم اعتبار الاطلاع على المعلومات المسجلة بالكمبيوتر مشكلا لجريمة من جرائم الأموال قد جاء على غرار ما هو مستقر بالنسبة للملفات الورقية من أن مجرد الاطلاع على تلك الملفات – مع تركها في مكانها – لا يشكل جريمة سرقة أو نصب أو خيانة أمانة [٢] .

ولا يبقى سوى توفير الحماية الجنائية ضد هذا السلوك من خلال نصوص خاصة أدخلتها العديد من التشريعات كالقانون الأمريكي وبعض القوانين الأوربية ، كالقانون الألماني [٣] ، حرصا على المصالح الاجتماعية التي يعتدي عليها أو يهددها مثل هذا السلوك وإدراكا من المشرع لحقيقة أن القواعد العامة لا تفي بتحقيق ذلك المأرب .

الوضع الرابع : إجراء توصيلات بالجهاز للحصول على المعلومة

---

(١) حكم صادر من محكمة الاستئناف في سنة ١٩٧٩ مشار إليه في :
Ultrich Sieber, The international Handbook on Computer Crime, John Wiley & Sons, New York , 1986, p. 54.

(٢) انظر:
Marise Cremona , Jonathan Herring MA , Criminal law , Macmilan , 1998, p. 234.

(٣) انظر :
Manfred Möhrenschlager , Computer Crimes and Other Crimes against Information Technology in Germany , Rev.int.dr.pén.1993,p.338.

يقوم المتهم – في هذا الوضع – بإجراء توصيلات على جهاز الكمبيوتر لمعرفة المعلومات الموجودة بالجهاز أو التي تصل إلى هذا الجهاز. ويتم ذلك بالطبع بدون علم صاحب الحق على هذه المعلومات . وقد يقوم المتهم بتسجيل هذه المعلومات لديه وقد يكتفي بالعلم بها دون تسجيلها .

وقد يتمثل سلوك المتهم في التجسس على نظام الكمبيوتر عن بعد دون إجراء توصيلات معينة ، وذلك بالاستعانة بوسائل إلكترونية متقدمة .

ولا يثير الوضع الأول مشكلة قانونية إذ إن صفة المال المنقول لاشك متوافرة بالنسبة للشريط والاسطوانة المعبأة بالمعلومات . كما لا يثير الوضع الثالث مشكلة قانونية حيث لا تتوافر صفة المال المنقول ، ولا يمكن توفير الحماية الجنائية إلاّ من خلال سن نصوص خاصة .

وبالنسبة للوضع الرابع فإن المتهم لا يقوم فيه بحيازة الشيء المسجل عليه المعلومات ، كما لا يقوم فيه بنسخ المعلومات التي يحوزها المتهم في دعامة مادية معينة . وبدلا من ذلك يتمثل نشاط المتهم في التجسس، سواء اتخذ ذلك شكل إجراء توصيلة معينة بالجهاز أو استعمال أجهزة إلكترونية في هذا التجسس. ولا يوجد نص يجرم التجسس إلاّ بالنسبة لأسرار الدولة العسكرية أو السياسية. ويبرهن هذا كله على عدم كفاية القواعد العامة في جرائم الأموال بحماية المعلومات المبرمجة.

وقد كان ذلك سببا فيما صدر من أحكام للقضاء الأمريكي استبعدت فيها وقوع جريمة السرقة ممن قام بنسخ برامج من كمبيوتر مملوك للغير وذلك عن بعد[1]. كما استبعدت تلك الأحكام وقوع السرقة على بيانات سرية

---

(١) انظر حكم صادر من المحكمة العليا لولاية كاليفورنيا في قضية :
Ward v The Superior Court of California (1972) .

تخص مرضى إحدى المستشفيات قام المتهم بنسخها عن بعد من أجهزة المستشفى[1]. وقد جاء حكم المحكمة مستندا إلى عدم اعتبار الومضات الإلكترونية من قبيل الأشياء المحسوسة التي ترد عليها جريمة السرقة[2].

بالنسبة للوضع الثاني ،الذي يتمثل بصفة خاصة في نسخ المعلومات، استشعرت المحاكم الأوربية – ومنها المحاكم الفرنسية – ضرورة توفير الحماية القانونية التي توفرها أحكام السرقة والنصب وخيانة الأمانة للمعلومات ، وذلك قبل أن تصدر تشريعات خاصة صريحة بذلك في هذه الدول.

وقد جاء اجتهاد هذا القضاء مستندا إلى الحجج التالية:

١- المعلومات تكتسب صفة المال لأن لها قيمة. وتحمي جرائم الأموال كل ما له قيمة . ويبين من أحكام القضاء اهتمامها بعنصر القيمة ، بحيث تعتبر مالا كل ما له قيمة يحرص صاحبها عليه ويترتب على سلب هذه القيمة حدوث أضرار فعلية لصاحبها . فالقيمة هي إذن عنصر أساسي في تحديد مفهوم الملكية وبيان عناصرها. من ذلك أن محكمة النقض المصرية قضت – في خصوص سرقة الخط التليفوني – " إن الخط التليفوني له قيمة مالية تتمثل في تكاليف الاشتراك والمكالمات التليفونية المستعملة. ومن ثم فإنه يجوز أن يكون محلا للسرقة في مفهوم المادة ٣١١ من قانون العقوبات. فإذا كان المتهم قد قام بتحويل مسار خط تليفون المجني عليه إلى منزله ، وظل يستعمله طوال مدة تعطله في منزل المجني عليه ، أي أنه تملك

(١) انظر حكم صادر من محكمة كولورادو Colorado court في قضية :
People v. Home Insurance Company (1979) .

(٢) انظر
Ultrich Sieber , The international Handbook on Computer Crime , John Wiley & Sons 1986, p. 55.

فعلا قيمة الاشتراك والمكالمات التليفونية التي استعملت منذ تعطله " [(١) (٢)].

٢- المعلومات من الأشياء ما دامت قيمتها لا تستمد فقط مما تمثله من أفكار ، بل تندمج مع الدعامة المادية التي تستند إليها (شريط أو اسطوانة) وتضفي عليها قيمة ، حتى ولو لم يقم المتهم بالاستيلاء على الدعامة المادية واكتفى بنسخ المعلومات [(٣)] . كالمستند الذي يكتسب قيمته مما دوّن به من معلومات. لذا فإن مجرد الاطلاع على المعلومات لا يعتبر اختلاسا على مال منقول [(٤)] ، ذلك أن المتهم لا يكون قد استولى على المعلومات وإنما يكون فعله مقتصرا على العلم بمحتوى تلك المعلومات [(٥)].

وقد حرص المشرع الفرنسي على أن يضمّن قانون العقوبات الجديد نصا بسرقة الطاقة . فتنص المادة ٣١١ -٢ عقوبات على أن " يعتبر في حكم السرقة اختلاس الطاقة بسوء نية إضرار بالغير " [(٦)] . وقد تبنى المشرع اللبناني وجهة النظر هذه عندما نص في المادة ٦٣٥ بعد تعديلها بالمرسوم الاشتراكي رقم ١١٢ بتاريخ ١٦ / ٩ / ١٩٨٣ على أن " .. تنزل الطاقات المحرزة منزلة الأشياء المنقولة في تطبيق النصوص الجزائية " [(٧)] .

---

(١) نقض ١٧ نوفمبر سنة ١٩٨٠ ، أحكام النقض س ٣١ رقم ١٩٤ ص ١٠٠٦ .

(٢) مع ذلك يستبعد القضاء الفرنسي وصف السرقة عن استعمال المكالمات التليفونية على نفقة الغير بدون رضاه

Crim 12 déc.1990, Bull.crim .n° 430, D. 1991. J. 364. .

(3) Crim. 3 mars 1992, Rev. sc. crim. 1993, p. 546l .

(4) Veron , Droit pénal spécial, Armond Colin, 1999, 197.

(5) Marie- Paule LUCAS DE LEYSSAC, " Une information seule est-elle susceptible de vol ou d'une autre atteinte juridique aux biens?" , D. 1985,chronique,43.

(6) " La soustraction frauduleuse d'energie au préjudice d'autrui est assimilée au vol" .

(٧) د. علي عبد القادر القهوجي ، " الحماية الجنائية للبيانات المعالجة إلكترونيا " أعمال مؤتمر " القانون والكمبيوتر والإنترنت " الذي نظمته كلية الشريعة والقانون بدولة الإمارات في الفترة من ١ - ٣ سنة ٢٠٠٠بالعين ، المجلد الثاني ص ٢٦ .

٣- المعلومات مال منقول، فهي تنتقل دون أن يصيبه التلف . ومن المعروف أن المنقولات تختلف بحسب طبيعتها فيما يتعلق بطريقة انتقالها . فمنها ما ينتقل باليد كالبضائع ومنها ما ينتقل عبر أسلاك كالكهرباء [١] . وكانت أحكام النقض الفرنسية قد استقرت منذ عام ١٩١٢ على وقوع السرقة بالاستيلاء على التيار الكهربائي بدون رضاء شركة الكهرباء أو بالحصول عليه خارج العداد [٢]. ومن هذه الأموال ما ينتقل بالتدوين عن طريق الفاكس أو غيره من الأجهزة كالنقود في البنوك . وتنتقل المعلومات بطرق مختلفة عبر دوائر أو يتم تسجيها في أشرطة أو اسطوانات. وما اختلاف المعلومات في أسلوب انتقالها إلاّ أن يكون تعبيرا عن الاختلاف في طبيعتها. فمما لا شك فيه أن الأمر يتعلق بصورة حديثة من صور الأموال المنقولة ، لها ، وهو ما يميزها عن غيرها من أموال.

٤- المعلومات مملوكة لصاحبها. لا شك يثور أن المعلومات ليست من الأموال المباحة ، بل إنها من المعلومات المملوكة للغير، مادام صاحبها يحرص على إخفائها عن الغير.

ويختلف الأمر لو أن صاحبها أتاح للغير العلم بها، كأن يبثها عبر شبكة الإنترنت مثلا . في هذه الحالة تكون هذه المعلومات مالا مباحا بالمعنى المعرّف به في جرائم الأموال. ومع ذلك فإن هذه المعلومات تبقى منسوبة إلى صاحبها وتتمتع بالحماية المقررة لحق المؤلف، مادامت قد توافرت شروط تلك الحماية.

(1) Bouzat, Infractions contre les biens , Rev .sc .crim. 1985, chronique de jurisprudence ,p. 879.
(2) Crim. 12 décembre 1984, Bull. Crim. 403, D. 25 avr. 1985, I. R. p. 186, Rev. sc. crim. 1985, p. 579, Crim. 11 oct. 1978, D. 1979, p. 76.

ومن الجلي أن برامج الحاسب الآلي يضعها صاحبها تحت تصرف الجمهور بعد دفع قيمتها لصاحب الحق في توزيعها. وبالتالي فإنه لا يتصور وقوع جريمة السرقة عليها . ولكن هذه البرامج تتمتع بالحماية المقررة في قانون حق المؤلف[1]، إذا قام المتهم بنسخها بغرض الاستغلال دون رضاء القائم بالتوزيع. ومع ذلك يبقى القيام بعمل نسخة للاستعمال الشخصي خارجا عن مجال التأثيم المقرر في قانون حق المؤلف. فتنص المادة ١٢ من قانون حماية حق المؤلف بعد تعديلها بالقانون رقم ٣٨ لسنة ١٩٩٢ على أنه "لا يجوز للمؤلف الذي نشر مصنفه بإحدى الطرق المبينة بالمادة (٦) من هذا القانون أن يمنع أي شخص من عمل نسخة وحيدة من هذا المصنف لاستعماله الشخصي وكذلك المصنفات السمعية والسمعية البصرية ، إذا تم إذاعتها كاملة بالإذاعة أو عرضها بالتليفزيون".

٥-المعلومات تصلح أن تكون محلا للحيازة. ولما كانت الحيازة هي سيطرة لشخص على الشيء ، فإن هذا المفهوم لا يتنافر مع المعلومات. هذه المعلومات تصبح في حيازة صاحب الحق في تلك الحيازة مادامت في جهازه أو في أشرطة أو اسطوانات خاصة به.

بيد أنه إذا لم تكن المعلومات مدوّنه على دعامة مادية ، فإن الأمر يتعلق بخدمات وليس بأموال. وبناء عليه إذا قام صاحب هذه المعلومات ببثها عبر شبكة معينة، وقام آخر باعتراضها بوسيلة أو بأخرى، كاستعمال كلمة السر مثلا بطريق الغش، فإن الأمر لا يتعلق بسرقة أو بنصب. ويرجع ذلك إلى عدم توافر صفة المنقول في المعلومات محل البث . فعلى الرغم من توافر

(١) د. على عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب ، دار الجامعة الجديدة للنشر، ١٩٩٧ ص ٢٣ .

سيطرة صاحب المعلومات محل البث عليها وذلك بربط الحصول عليها باستعمال كلمة السر بما يصح معه القول بتوفر الحيازة لهذه المعلومات، فإن جريمة السرقة لا تقع وكذلك لا تقع جريمة النصب، وذلك لانتفاء صفة المنقول.

٦- لا يتنافر اعتبار المعلومات من المنقولات مع السوابق القضائية التي اعتبرت من قبيل المنقولات ما قام به المتهم من الحصول على فترة زمنية للوقوف بسيارته في موقف السيارات وذلك بالاستعانة بقطعة معدنية ليس لها قيمة. فقد اعتبرت محكمة النقض الفرنسية ذلك مشكلا لجريمة النصب[١]. والمعروف أن هذه الجريمة لا تقع إلا على المنقولات. كما سبق وأن اعتبرت محكمة النقض المصرية من قبيل السرقة قيام المتهم باستعمال التليفون (الخط الدولي) دون رضاء صاحبه[٢].

٢٤- النتائج القانونية المترتبة على اعتبار المعلومات منقولات:

يترتب على اعتبار المعلومات المسجلة على دعامة مادية من المنقولات نتائج قانونية هامة أهمها:

١- المعلومات المسجلة تعتبر من المنقولات:

٢٥ - تعتبر المعلومات المسجلة على دعامة مادية (في جهاز الكمبيوتر أو على شريط أو اسطوانة) من المنقولات التي تصلح أن تكون محلا للسرقة أو النصب أو خيانة الأمانة ، حتى ولو لم يقم المتهم بالاستيلاء على تلك الدعامة المادية، كأن يكتفي بنسخ تلك المعلومة . وقد انتهت أحكام القضاء الفرنسي إلى ذلك بعد أن تغلبت على صعوبتين: الأولى تتعلق بتحديد مفهوم

---

(1) Crim.10 déc. 1970, J.C.P.1972. II. 17277, D. 1972, p. 155.

(٢) نقض ١٧ نوفمبر سنة ١٩٨٠ ، أحكام النقض س ٣١ رقم ١٩٤ ص ١٠٠٦ .

المنقول، والثانية تتعلق بتحديد مفهوم الاختلاس، بحيث يتمشى مع التطور في تقنية المعلومات[1].

ومع ذلك فإنه يبين من أحكام القضاء الفرنسي أن جرائم الأموال لا يكون لها محل إذا لم تكن المعلومات مسجلة على دعامة مادية (كما في حالة اعتراض برامج كانت محلا للبث عبر الأثير)[2].

٢ - إخفاء المعلومات إخفاء لأشياء مسروقة:

٢٦ - على التساؤل التالي: هل تصلح المعلومات المنسوخة أو المصورة على دعامة مادية أن تشكل محلا لجريمة الأشياء المسروقة ؟ كان رد القضاء الفرنسي بالإيجاب[3]. فقد وجه الاتهام على هذا الأساس لصحفي قام بنشر صورة مستندات لا توجد إلاّ في مصلحة الضرائب وتتعلق بدخل أحد المسئولين في إحدى الشركات. ولم يتمكن التحقيق من معرفة الشخص الذي قام بتصوير هذه المستندات الضريبية إخلالاً بسر المهنة الذي يفرضه عليه القانون بسبب طبيعة عمله في مصلحة الضرائب. قضت المحاكم الفرنسية بإدانة الصحفي بجريمة إخفاء أشياء مسروقة أو متحصلة من جريمة. وقد جاء حكم المحكمة مستندا إلى أن إخفاء للمعلومات المصورة ضوئيا بعد التوصل إليها بطريق ارتكاب جريمة إفشاء سر المهنة يُعد إخفاء لمنقول في مفهوم تلك الجريمة. فقد ظهر للمحكمة في هذه القضية أن مجهولا يعمل في مصلحة الضرائب قام بتصوير هذا المستند وأرسله إلى الصحفي المتهم الذي قام بنشر صورته في صحيفته[4]. وقد عُنيت المحكمة في هذا الحكم بالقول بأن محل

---

(١) انظر لاحقا ٣٢ .

(٢) انظر لاحقا رقم ٢٩.

(3)Reynald OTTENHOF , Infractions contre les biens, chronique de jurisprudence, Rev.sc.crim.1996, p.658.

(4) Crim. 3 avril 1995 J.C.P. 1995. II. 22429, Gaz, Pal. 24, 25 mai 1995, Rev. sc. crim. 1995, 599, Crim.26 oct. 1995, Bull. crim.n. 324, Rev. sociétés 1996, p. 326.

الإخفاء ليس هو المعلومات في حد ذاتها ولكن الصورة الضوئية للمستند الذي يحوي المعلومات[1].

وقد جاء هذا الحكم في نفس الاتجاه الذي سبق أن اتخذته محكمة النقض الفرنسية عندما أيدت حكما بإخفاء أشياء مسروقة صدر على من قام بتقديم صورة ضوئية لمستندات تتعلق بسياسة التوظيف في الشركة في إحدى الدعاوى، وكانت هذه المستندات قد تمت سرقتها من الغير بغرض تصويرها[2].

وقد خطت أحكام القضاء خطوه أوسع عندما قضت بأن إخفاء المعلومات المتحصلة من نسخ شريط أو اسطوانة أو من الجهاز نفسه يشكل جريمة إخفاء لأشياء مسروقة ما دام المتهم لم يكن مخولا بنسخ هذه المعلومات. فالمعلومة وفقا لأحكام ذلك القضاء هي من قبيل المال المنقول في حكم جريمة إخفاء الأشياء المسروقة أو المتحصلة من جريمة. لكن ذلك مشروط بتواجدها على دعامة مادية (شريط أو اسطوانة أو ورقة) .

ولكن ذلك القضاء لم يستقر إلاّ بعد اضطراب شهدته بعض الأحكام بسبب الطبيعة المعنوية لبعض الأموال. فقد سبق أن قضت محكمة النقض الفرنسية بوقوع جريمة إخفاء أشياء مسروقة ممن قام بتلقي سر الصنعة من أحد العاملين بإحدى الشركات وقام باستغلاله لمصلحته[3]. هذا القضاء كان محلا للانتقاد من جانب الفقه[4].

---

(1) Reynald OTTENHOF, Infractions contre les biens, Rev.sc.crim. 1995, p. 820.
(2) Arrêt U.C.I.P., Crim. 12 janv. 1981, Bull.crim.,n.15, p.58.
(3) Arrêt Maillot, crim. 7 nov. 1974 , Bull. crim. N. 323 , D. 1974 .somm. 144, Gaz.Pal.1975.I.somm.96.
(4)Marie–Paule LUCAS DE LEYSSAC, op.cit.,p.49; Jacques FRANCILLON , Rev.sc. crim.1995, op.cit., p.602.

فالأموال المعنوية البحتة ، أي التي ليس لها دعامة مادية تأخذ حكم المنافع التي لا ترد عليها جرائم الأموال التقليدية (سرقة – نصب – خيانة أمانة – إخفاء الأشياء المسروقة) . لذا كان مقبولا أن حكم القضاء الفرنسي بعدم وقوع جريمة إخفاء الأشياء المسروقة إذا كان ما نسب إلى المتهم أنه ركب سيارة مسروقة مع علمه بسرقتها [1] .

وقد طبق القضاء الفرنسي وصف إخفاء الأشياء المتحصلة من جريمة على ما قام به مدير مكتب أحد المسئولين من استقبال صور تمثل ممارسة للشذوذ الجنسي مع الأطفال وتخزينها في الجهاز التابع لتلك الجهة العامة[2]. وقد انتهت المحكمة في تلك القضية إلى وقوع جريمة إفساد قاصر (أقل من ١٥ عام) التي نص عليها القانون الفرنسي . وليس يعني هذا القضاء اعتبار الصور بمثابة أموال يسري عليها تجريم الإخفاء، ولكن ذلك يعني أن تلك الصور تكتسب هذه الصفة من اللحظة التي تسجل فيها على دعامة مادية.

٣ – وقوع جريمة الإتلاف على المعلومات المبرمجة :

٢٧ – مادامت المعلومات المبرمجة سواء في الكمبيوتر أو في شريط أو اسطوانة من المنقولات[3]، ومادام التدخل بمحو أو بتشويه هذه المعلومات يرقى إلى درجة إتلافها ، فإنه لا شيء يحول دون القول بوقوع جريمة

---

(1) Crim. 9 juill. 1970, Bull. crim. n° 236; D. 1971, p. 3; J.C.P. 1971, II. 16616.

(2) T. corr. Mans , 16 fev. 1998, in " Responsabilité pénale d un utilisateur : détournement d un ordinateur à usage professionnel pour récéler des images pédophiles , J. C.P. 1999. II. 10011.

(٣) د. هشام محمد فريد رستم ، المرجع السابق ص ٣١٣ ؛ د. هدى حامد قشقوش ، الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني ، بحث مقدم إلى مؤتمر " القانون والكمبيوتر والإنترنت " ، كلية الشريعة والقانون بدولة الإمارات ،مايو ٢٠٠٠ ، الجزء الأول ص ١٠ .

الإتلاف على هذه المعلومات[1]. ويستوي عندئذ في الإتلاف أن يكون كليا أو جزئيا[2].

فلم يكن غريبا لذلك أن اتجه التفسير القضائي في بعض الدول إلى وقوع جريمة الإتلاف على البرامج والمعلومات. من ذلك ما انتهت إليه المحكمة العليا في النمسا ، قبل صدور القانون الخاص بالكمبيوتر الذي تضمن جريمة العبث بالمعلومات المبرمجة في سنة ١٩٨٧[3].

وقد تبنى هذا الاتجاه تشريعات أوربية منها القانون النمساوي [4] والقانون الدانمركي [5] والقانون اليوناني [6] والقانون الإيطالي [7] والقانون الهولندي [8] والقانون النرويجي والقانون الإنجليزي [9] بالإضافة إلى القانون الكندي .

---

(١) د. على عبد القادر القهوجي ، المرجع السابق ، ص ٧٩ ؛ د. هدى حامد قشقوش ، " الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني ، مؤتمر جامعة الإمارات ، كلية الشريعة والقانون حول " القانون والكمبيوتر والإنترنت " ، في الفترة ١- ٣ مايو سنة ٢٠٠٠ ص ٨ .

(٢) د. عمر الفاروق الحسيني ، تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي ، مؤتمر جامعة الكويت حول " القانون والحاسب الآلي " ، مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي ، ١٩٩٤ ص ٩١ .

(٣) انظر :

Peter J. Schick0 , Gabriele Schmölzer, Computer Crimes and Other Crimes against Information Technology in Austria , in " Delits informatiques et autres infractions à la technologie de l'information " , Colloque préparatoire , Rev. int. dr. pén. 1993,p.147.

(٤) انظر section ١٢٥ من قانون العقوبات النمساوي .

(٥) انظر section ٢٩١ من قانون العقوبات الفنلندي .

(٦) انظر section ٣٨١ من قانون العقوبات اليوناني .

(٧) انظر section ٤٢٠ and ٦٣٥ من قانون العقوبات الإيطالي .

(٨) انظر section ٣٥٠ من قانون العقوبات الهولندي .

(٩) انظر The Criminal Damage Act ١٩٧١ .

فبينما يستند تجريم إتلاف البيانات إلى تفسير قضائي للنصوص العامة في بعض التشريعات ، فإن هناك من التشريعات ما يورد نصوصا خاصة لمثل هذا التجريم ليواجه الطبيعة الخاصة لبيانات الكمبيوتر. من ذلك أن قانون عقوبات ولاية واشنطن بالولايات المتحدة الأمريكية قد نص على أن الإتلاف المادي يشمل " تغيير أو إتلاف أو مسح الملفات والمعلومات والبيانات وبرامج الكمبيوتر "[١].

بيد أن ذلك لم يسلم من مناقشة ، قوامها أن الإتلاف جريمة تقع على شيء مادي ، بينما المعلومات ذات طبيعة معنوية . لذا فإن بعض التشريعات الأوربية لا تعتبر مجرد مسح البيانات - دون الإضرار المادي بالنظام - مشكلا لجريمة الإتلاف. من تلك التشريعات القانون البلجيكي [٢] والقانون الفنلندي.

وحسما لمظنة الخلاف في التفسير، أورد قانون العقوبات الفرنسي نصا خاصا بتجريم الإخلال بنظام الكمبيوتر[٣] . فتنص المادة ٣٣٢- ٢ من قانون العقوبات على أن " يُعاقب كل من يقوم بإعاقة أو إحداث الاضطراب في عمل نظام المعلومات المبرمجة بالحبس مدة ثلاث سنوات وبغرامة مقدارها ٣٠٠ ألف فرنك ".

ويسري هذا النص على استعمال فيروس، أيا كان أثره ، مادام أنه يؤدي إلى اضطراب في عمل الكمبيوتر. فلا يلزم في الفيروس أن يكون من

---

(1) " the alteration , damage , or erasure of records , information , data or computer programs which are electronically recorded for use in computers " .

(٢) انظر section ٥٢٨ and ٥٥٩ من قانون العقوبات البلجيكي .

(٣) د. عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، ١٩٩٥ ص٧٢.

شأنه مسح جميع المعلومات أو جزء منها. بل يسري نص التجريم على كل برنامج يسبب خللا بنظام عمل الكمبيوتر. ويعد من قبيل هذا الخلل البطء في سير الجهاز أو تقليل كفاءته.

٤- عدم وقوع جرائم الأموال على وقت الكمبيوتر:

٢٨ - قد يستعمل أحد الأشخاص جهازا للكمبيوتر ينتمي إلى الغير دون رضائه، وقد يكون الأول مستخدما لدى الأخير يستعمل الجهاز بعد مواعيد العمل الرسمية . هذا الاستعمال يهدد مصالح لصاحب الجهاز : منها سرية المعلومات التي يحتويها الجهاز أو إضافة أعباء مادية بسبب هذا الاستعمال .

فقد ظهرت بظهور الكمبيوتر قيمة الوقت عند استعمال الكمبيوتر ، وذلك بالاستفادة من الخدمات التي يؤديها ذلك الجهاز والتي لها قيمة مالية[١]. من ذلك الاستفادة بشبكة الإنترنت ما تقدمه من معلومات وكذلك ما تقدمه بعض الشركات من برامج أو بعض القنوات من بث تليفزيوني معين .

في هذا الفرض يصعب توفيق هذا الوضع مع القواعد العامة والقول بالسرقة المؤقتة أو بالظهور بمظهر المالك ، خاصة وأن الأمر يتخذ شكل الخدمة أو المنفعة وليس المال المادي [٢] . فمن المقرر أن جرائم الأموال لا ترد على الخدمات أو المنافع [٣]. ولا يبقى سوى الاعتراف بالمعلومات باعتبارها من الأموال المنقولة مادامت مسجلة على دعامة مادية وكذلك الاعتراف بالوقت باعتباره من القيم المنقولة المعنوية ما دام هذا الوقت يتعلق

---

(١) د. محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ١٩٩٤ص ٨٥ .

(2) Arrêt Giuesppe Sacchi , 30 avril 1979,Recueil de la jurisprudence de la Cour, p. 409.

(3) Bouzat , Infractions contre les biens, Rev.sc.crim 1987, chronique de jurisprudence, p. 211.

بوسيلة حدد صاحبها مقابلا لاستعمالها . فلم يعد المال مقتصرا في مفهومه على المال المادي ، بل انضمت إليه طائفة حديثة من الأموال المعنوية ساهم جهاز الكمبيوتر في إيجادها وتسليط الضوء عليها.

والحقيقة أن اللجوء إلى الآلة قد ساهم في إبراز الوقت كقيمة منقولة . فالوقت الذي تستغرقه المكالمة التليفونية قيمة مالية منقولة اعتبرته محكمة النقض المصرية مالا منقولا يحميه تجريم السرقة، على ما سبق بيانه. ووقت انتظار السيارة في موقف السيارات المدفوع الأجر باستعمال قطعة معدنية بدلا من العملة المطلوبة اعتبرته محكمة النقض الفرنسية منقولا يحميه تجريم النصب[1]. وقد دعا ذلك البعض إلى اعتبار الوقت مالا وبالتالي فإن استخدام الآلات في أثناء وقت معين تقع به جريمة سرقة المنفعة vol d'usage [2].

ونظرة إلى أحكام القانون الإنجليزي ، نجد أن قانون السرقة لسنة ١٩٧٨ في الفصل الأول منه ينص على أن يرتكب الجريمة كل شخص يحصل على خدمات من الغير باستعمال التدليس (الفقرة الأولى). كما تنص الفقرة الثانية من القانون ذاته على أن الحصول على خدمات يتم بطريق التدليس إذا أوهم المتهم الغير أنه أدى له الأجر المطلوب أو أنه سوف يؤدى له ذلك الأجر في نظير تلك الخدمة[3]. وقد تضمن تعديل قانون السرقة في إنجلترا إشارة واضحة إلى الخدمات باعتبارها محلا لجريمة السرقة والتدليس[4].

---

(1) Crim. 10 décember 1970, J.C.P. 1972. II. 17277, D. 1972,.p. 155 .

(٢) انظر : أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، رسالة ، طنطا ، ص ٥٧٨ .

(3) Section (1) of Theft Act 1978 provides : (1) A person whom by any deception dishonestly obtains services from another shall be guilty of un offence ,
(1) It is an obtaining of services from where the other is induced to confer a benefit by doing some act, or causing or permitting some act to be done , on the understanding that the benefit has been or will be paid for

(4) Reed, Seago , Criminal law, éd. Sweet and Maxwell, 1999, p. 440 .

هذا النص العام في القانون الإنجليزي يلائم الوضع الخاص للبرامج وغيرها من الخدمات التي تقدمها جهات البث عن طريق الأجهزة المختلفة ومنها أجهزة الكمبيوتر.

وقد اتجهت بعض التشريعات الأوربية إلى العقاب على سرقة وقت الكمبيوتر (أي سرقة خدمة الكمبيوتر) theft of service . وقد أرجعته بعض التشريعات إلى النص العام الذي تعرفه والذي يعاقب على الاستعمال غير القانوني أو غير المصرح به لملكية الغير unauthorized or illegal use of another's property [(١)] . وواضح أن هذا النص الأخير هو من النصوص العامة التي يمكن تطبيقها على إساءة استعمال الكمبيوتر . من هذه التشريعات التي تتبنى هذا النص القانون البلجيكي [(٢)] والقانون الدانماركي[(٣)] والقانون الفنلندي [(٤)] .

لكن تشريعات أوربية أخرى لا تجرم استعمال الشيء المملوك للغير بدون رضائه إلا على سبيل الاستثناء كما في حالة استعمال سيارة الغير مثل القانون الفرنسي والقانون الألماني [(٥)] والقانون المصري. كما أنها لم تدخل نصوصا خاصة للعقاب على استعمال خدمة الكمبيوتر بطريقة غير قانونية . من هذه التشريعات الأخيرة القانون النمساوي والقانون الياباني والقانون الإنجليزي[(٦)].

---

(١) انظر

Ulrich Sieber, id, at 81 .

(٢) انظر section٤٦١ من قانون العقوبات البلجيكي .

(٣) انظر section٢٩٣ من قانون العقوبات الدانمركي .

(٤) انظر section٢٩٣ من قانون العقوبات الفنلندي .

(٥) انظر

Manfred Möhrenschlager, Computer Crimes and Other Crimes against Information Technology in Germany , Rev.int.dr.pén. 1993, p. 345 .

(٦) انظر

Ultrich Sieber, id , at 81.

لذا أدخلت معظم الولايات الأمريكية تشريعات تعاقب على سـرقة الخدمات theft of services . وقد اعتبر قانون جـرائم الكمبيـوتر في ولايـة فرجينيا Virginia لسنة ١٩٨٤ أن وقت الكمبيوتر أو الخدمات التي يؤديهـا أو البيانات المبرمجة داخله [١] تعتبر من قبيل المـال المنقـول المملـوك للغـير الذي تقع السرقة باختلاسه [٢] . فقد نص هذا القانون السابق صراحة على عقاب " كل شخص يستعمل - عمدا - كمبيوتر أو شبكة كمبيوتر قاصـدا الحصول مـن وراء ذلـك علـى خدمـة مـن خـدمات الكمبيـوتر دون وجـه حق "[٣]. ويعاقب قانون جرائم الكمبيـوتر لـسنة ١٩٨٨ في ولايـة فلوريـدا على استعمال كمبيوتر الغير دون رضـاه ، كمـا يعاقـب علـى عـدم تمكـين صاحب الحق في استعمال خدمات الكمبيوتر مـن ذلـك الاسـتعمال بـدون وجه حق [٤]. كما أن تعديل قانون العقوبات الكنـدي لـسنة ١٩٨٥[٥] قـد تضمن نصا خاصا يعاقب على سرقة خدمات الكمبيوتر [٦].

---

(1) " Computer time or services or data processing services or information or data stored in connection therewith " .

(٢) انظر Ultrich Sieber, id, at ٨٣

(٣) انظر s. ١٨,٢ من قانون جرائم الكمبيوتر في فرجينيا لسنة ١٩٨٤ :

" Any person who willfully uses a computer or a computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services, which shall be punishable as a class 1 misdemeanor".

(٤) انظر الباب ٨١٥ من قانون جرائم الكمبيوتر في ولاية فلوريدا :

" Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer , computer system , or computer network , or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services , which, in whole or part , is owned by, under contract to , or operated for, on behalf of, or in conjunction with another commits an offense against computer users " .

(5) section 301.2 .

(٦) انظر

Ulric Sieber, id at 83.

ونظرا لما قد يثار حول قيمة الوقت ومدى اكتسابه صفة المال المنقول وبسبب النظرة إلى الوقت بوصفه خدمة أو منفعة معينة ، كان من الضروري إدخال نصوص تشريعية خاصة للعقاب على هذا النوع من التداخل في المعلومات المرسلة والبرامج المشفرة ، على ما سيلي بيانه .

وحقيقة الأمر أن التداخل في نظام الكمبيوتر الذي ينتمي إلى الغير دون رضاه هو نوع من استعمال هذا النظام في غالبية الأحوال[1]. بيد أن التداخل يتسع مجال تطبيقه أكثر من مجرد الاستعمال. فقد يحدث التداخل عن بعد دون تشغيل الجهاز وقد يحدث والجهاز في حالة تشغيل ويكون ذلك للاطلاع على ما بالجهاز من بيانات.

وعلى الرغم من غياب نص صريح بتجريم التداخل في بعض التشريعات ، فإن للقضاء أن يجتهد في تطبيق القواعد العامة والتوصل إلى وقوع جريمة السرقة على الجهاز في أثناء وقت استعماله ، أي اللجوء إلى فكرة الاختلاس المؤقت[2].

٥- عدم وقوع السرقة على البرامج المشفرة:

٢٩ – ترسل بعض القنوات الخاصة برامج مشفرة يملك المستقبل مشاهدتها في نظير اشتراك سنوي. وتقوم الشركة التي تبث الإرسال بتزويد المشتركين بالأجهزة المناسبة لحل الشفرة حتى يتمكنوا من استقبال الإرسال أو تحسين صورة هذا الإرسال. وقد قام البعض باستعمال أجهزة مقلدة حتى

---

(١) انظر د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، المرجع السابق ص ٢٨١ .

(٢) انظر

Xavier Linant de Bellefonds , Alain Hollande, Pratique du droit de l'informaftique, éd. Delmas 1989, p. 243.

يتمكنوا من استقبال تلك البرامج بصورتها المحسنة دون دفع الاشتراك فيها.

انتهت أحكام القضاء الفرنسي إلى عدم وقوع جريمة السرقة في هذه الحالة [1] وصدرت أحكام بالبراءة [2] ، وذلك قبل أن يتدخل المشرع الفرنسي بسن قانون خاص ليعاقب على ذلك الفعل بنص خاص وليس بوصف السرقة، تفاديا لاضطراب المحاكم في التفسير في إجابتها على التساؤل التالي: هل البرامج مال منقول ؟

فمع أن المعلومات مال له قيمة، إلاّ أنه في مقام جرائم الأموال لا تصبح محلا للتجريم إلاّ إذا كانت مسجلة على دعامة مادية . والأمر ليس كذلك بالنسبة للبرامج التي تبثها إحدى الشبكات[3]. وقد استبعدت محكمة استئناف باريس اعتبار البرامج المرسلة عبر الأثير بمثابة التيار الكهربائي أو تصوير المستندات أو البيانات المبرمجة في الكمبيوتر[4]. كما استندت المحكمة – في نفيها لوقوع جريمة السرقة – إلى عدم توافر الاختلاس في هذه الواقعة ، حيث لم يتجرد المالك من الإرسال الذي يقوم ببثه . كما أنه لم يكن من شأن سلوك المتهم إحداث اضطراب في استلام المشتركين لصورة الإرسال الذي كان يصلهم . كما استبعدت المحكمة – في هذا الحكم – وقوع جريمة التحريض على ارتكاب الجرائم بطريق الصحافة ، على سند من عدم وقوع جريمة أصلا عندما نشر الصحفي مقالا يدعو فيه القراء إلى مشاهدة إرسال

---

(1) Cour de Paris, Aff. Canal Plus, arrêt du 24 juin 1987 , Gaz. Pal. 1987 .2. 512, Rev .sc.crim.1987.p. 211.

(2) Jean Pradel, Michel Danti- Juan, Droit pénal spécial, éd. Cujas , 1995,p.544.

(3) Jacques FRANCILLON," infractions relevant du droit de l'information et de la communication," , Rev. sc. crim. 1995 ,Chronique de la jurisprudence , p. 602.

(٤) انظر

Jérôme Huet, Herbert Maisl, Droit de l'informaftique et des télécommunications, éd. Litec, p. 866.

إحدى القنوات المشفرة باستعمال جهاز بسيط يمكن الحصول عليه بسعر زهيد ، بدلاً من دفع الاشتراك إلى هذه القناة الخاصة[١].

وقد حدا ذلك بالمشرع إلى معالجة القصور في القواعد التقليدية في قانون العقوبات بتدخله بتشريع خاص لحماية هذا النوع من البث، حرصا على استمرار هذه الخدمة لصالح جمهور المشاهدين. فقد صدر القانون رقم ١٠ لسنة ١٩٨٧ وتم تعديله بمقتضى القانون الصادر في ١٦ ديسمبر سنة ١٩٩٢ الذي أدخل في قانون الصحافة والاتصال المواد ٧٩ -١ و٧٩ -٢ و ٧٩- ٣ [٢] . وتعاقب المادة الأولى على التصنيع أو الاستيراد - بغرض البيع أو الإيجار - أو الحيازة بغرض البيع لمواد أو تجهيزات الغرض منها استقبال برامج تليفزيونية لا تتاح إلا بناء على اتفاق مع الشركة المرسلة لها. وتعاقب المادة الثانية على الإعلان عن مثل هذه المواد والتجهيزات المشار إليها في المادة السابقة . وتعاقب المادة الثالثة على إعادة بث الإرسال الذي يستقبله أحد المشتركين إلى الغير الذي لم يحصل على موافقة الشركة المرسلة ، إضرارا بحقوق تلك الشركة . وقد بدأ القضاء الفرنسي في تطبيق هذه الأحكام لحماية تلك البرامج بمقتضى تلك النصوص الخاصة [٣].

٣٠- الموقف الخاص بسرقة الحقوق المالية في بعض التشريعات:

لا تتنافر الطبيعة الخاصة للمعلومات مع ما هو معمول به في بعض التشريعات - مثل القانون الإنجليزي - التي تسمح بوقوع جريمة السرقة على

---

(١) انظر

Cour de Paris 24 juin 1987 , D. 1988. somm. 226 .

(2) Jacaues FRANCILLON, Infractions relevant du droit de l'information et de la communication, Rev.sc.crim. 1993, chronique de jurisprudence , p. 562.

(3) Crim, 23 mars 1992, B. n. 124 , 19 aout 1992 , B. n. 277, Rev. sc.crim.1993 , p. 563.

الأموال المعنوية . فالسرقة تقع وفقا لهذا القانون على الحقوق chose in action [١] وغيرها من الأموال المعنوية . ويعرف ذلك النوع من الأموال chose in action بأنه حقوق يمكن حمايتها عن طريق دعوى قضائية. تطبيقا لذلك قضي في إنجلترا بوقوع السرقة ممن قام ببيع رخصة تصدير بضاعة إلى الخارج تنتمي إلى شخص آخر [٢]. ومن التطبيقات القضائية على سرقة الحقوق ما قضي به في إنجلترا من وقوع الجريمة ممن زور شيكات على حساب معين في أحد البنوك . وتقع الجريمة عندئذ بمجرد تقديم الشيك إلى البنك لأن ذلك يدل على أن المتهم تملك الحق في سحب الرصيد [٣] . بيد أن المعلومات لا تعتبر منتمية إلى طائفة الحقوق والدعاوى rights and claim[٤].

وقد تبنى القانون الأسترالي نفس الاتجاه عندما اعتبر قانون عقوبات ولاية فكتوريا [٥] Victoria – على غرار القانون الإنجليزي بشأن السرقة Theft Act لسنة ١٩٦٨ – مالا منقولا محلا للسرقة " النقود وكل الأموال المنقولة العينية أو الشخصية وكذلك الحقوق والأموال غير المادية " [٦] .

على الرغم مما قد يبدو أنه يمكن إدخال المعلومات في زمرة الأموال المعنوية وفقا للقانون الإنجليزي ، فإنه من اللازم توافر نية التملك أيضا لدى المتهم للقول باقترافه جريمة السرقة . لذا قضي في إنجلترا بعدم وقوع السرقة

(1) Section 4 (1) of Theft Act provides that " Property includes money and all other property, real or personal including thing in action an other intangible property " .
(2) All. Gen. For Hong Kong v. Nai Keung (1987)
(3) Khan (1979) .

(٤) انظر

Martin Wasik , Computer Crimes and Other Crimes against Information Technology in the United Kingdom , Rev.int.dr.pén.1993,p.629 .

(5) Section 71 of the Victorian Crimes (theft) Act 1973 .
(6) " money and all property real or personal including things in action an other intangible property " .

من طالب قام باختلاس ورقة الامتحان وتصويرها وإعادتها إلى مكانها ، استنادا إلى توافر نية الرد الفوري لديه ، مما يجعل الأمر من قبيل الاستعارة بدون إذن صاحب الحق في الشيء[1].

٣١- الازدواجية في تحديد الطبيعة القانونية المعلومات المبرمجة :

تتفق التشريعات المختلفة على أن المعلومات المبرمجة تنسحب عليها الحماية القانونية المقررة لحق المؤلف ، مادامت شروط هذا الحق قد توافرت وأهمها شرط الابتكار[2]، عندما تتخذ هذه المعلومات وصف البرامج.

ولم يعد الأمر يشكل اجتهادا من الفقه أو من القضاء للقول بانسحاب تلك الحماية على برامج الكمبيوتر. فقد أصبحت التشريعات المعاصرة تتضمن نصا صريحا بذلك. فتنص المادة (٢) من قانون حق المؤلف رقم ٣٥٤ لسنة ١٩٥٤ المعدل بالقانون رقم ٣٨ لسنة ١٩٩٢ على أن : تشمل الحماية المنصوص عليها في هذا القانون مؤلفي : - مصنفات الحاسب الآلي من برامج وقواعد وبيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة ". كما تتفق التشريعات الأمريكية والأوربية على أن برامج الكمبيوتر تتمتع بالحماية القانونية المقررة لحق المؤلف، سواء في الجوانب المدنية لتلك الحماية أو في جوانبها الجنائية [3] . كما تضمن القانون رقم ٦٤ لسنة ١٩٩٩ في الكويت نصا (المادة الثانية) على حماية مصنفات الحاسب الآلي بمقتضى القانون السابق في شأن حقوق الملكية الفكرية (حق المؤلف).

ومع ذلك فإن أحكام القضاء استشعرت الحاجة إلى حماية المعلومات المبرمجة أي المتواجدة داخل جهاز الكمبيوتر أو المسجلة على شريط أو اسطوانة من نسخها دون رضاء صاحبها. وقد ترتب على هذا الاتجاه أن

---

(1) Oxford v. Moss (1979) .

(٢) د. محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسب الإلكتروني ، دار الثقافة ، ١٩٨٧ص ٢٧.

(٣) د. محمد حسام محمود لطفي ، المرجع السابق ص ١٥٥ .

بدأت الأحكام القضائية في إضفاء صفة المنقول على هذه المعلومات، وصولا إلى حمايتها من السرقة والنصب وخيانة الأمانة ، على غرار غيرها من الأموال المنقولة .

ومؤدى هذا الاتجاه أن ظهر التعارض بين صفة المعلومات المبرمجة بوصفها من الأفكار التي تستفيد من حق المؤلف وصفة المال المنقول الذي يكتسب الطابع المادي باعتباره من الأشياء.

ولم يرتفع هذا التعارض عندما تدخل المشرع في عديد من الدول وخاصة في الولايات المتحدة الأمريكية وفي الدول الأوربية المختلفة وذلك بتعديل أحكام السرقة والنصب وخيانة الأمانة لكي تشمل المعلومات بوصفها من الأموال المنقولة.

ويزداد الأمر تعارضا، إذ ا ما تذكرنا أن المشرع في تشريعات عديدة اعتبر المعلومات المبرمجة من المحررات، وذلك حتى يحميها من العبث بها . ومؤدى ذلك أن هذه المعلومات ليست مجرد أفكار يحميها حق المؤلف وليست مجرد أموال منقولة تحميها أحكام السرقة والنصب وخيانة الأمانة، ولكنها أيضا محررات تنسحب عليها أحكام التزوير. ويطرح التساؤل نفسه: هل المعلومات أفكار أم هي أموال منقولة أم هي لا هذا ولا ذاك بل هي من المحررات ؟

وخلاصة ذلك أنه للخروج من التناقض بين اعتبار البرامج والمعلومات من الأفكار وحمايته بالتالي بقانون حق المؤلف وبين اعتبارها من الأموال وحمايتها بالتالي بنصوص جرائم الأموال ، واعتبارها أيضا من المحررات وحمايتها بتجريم التزوير في المحررات ، فإنه من الواضح إيراد نصوص خاصة للحماية الجنائية وعدم التعويل على القواعد التقليدية في قانون العقوبات وقانون حق المؤلف .

الفرع الثاني

صعوبة القول باختلاس المعلومات

٣٢- اختلاف اختلاس المعلومات عن اختلاس المنقولات الأخرى:

واجه القضاء الفرنسي ، للقول بوقوع السرقة على المعلومات ، صعوبتان قانونيتان : الأولى تتمثل في اعتبار المعلومات من المنقولات . وقد حل هذا القضاء تلك المشكلة باعتبار المعلومات مالا منقولا مادامت مسجلة على دعامة مادية [١]. بدون ذلك لا تعتبر سوى أفكار معنوية بحتة لا يحميها التجريم المقرر في جرائم الأموال[٢].

بيد أن هذا القضاء كان لزاما عليه أن يتخطى صعوبة قانونية أخرى تتمثل في تحديد مفهوم الاختلاس في جريمة السرقة لكي يتلاءم مع طبيعة نسخ المعلومات . ذلك أن نسخ المعلومات المبرمجة لا يتضمن خروجها من حيازة صاحبها[٣]. ومن المستقر عليه أن الاختلاس بالمعنى التقليدي في جريمة السرقة يقتضي خروج المال من حيازة المجني عليه إلى حيازة الفاعل[٤]. لذا تستقر الأحكام القضائية على وقوع السرقة تامة بخروج الشيء المسروق من حيازة المجني عليه إلى حيازة الجاني. أما قبل ذلك فإن الأمر يتعلق بشروع في

---

(١) د. عمرو إبراهيم الوقاد ، الحماية الجنائية للمعلوماتية ، مجلة روح القوانين أبريل ١٩٩٨ ص ١١ .

(٢) انظر

Jacques FRANCILLON , Les crimes informatiques et autres crimes dans le domaine de la technologie informatique en France , Rev. int. dr. pén. 1993, p.305.

(٣) د. عمر الفاروق الحسيني ، " لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات " بحث مقدم إلى مؤتمر " القانون والكمبيوتر والإنترنت " مايو ٢٠٠٠ ، الجزء الأول ص ٢٣ .

(٤) د. مراد رشدي ، الاختلاس في جرائم الأموال ، مكتبة نهضة الشرق ١٩٨٦، ص ٣٣.

سرقة إذا بدأ المتهم في إخراج هذا الشيء من حيازة المجني عليه مع توافر نية التملك[1]. كما لا يتحقق وصف السرقة أيضا إذا كان المال في حيازة المتهم أصلا ثم استولى عليه لنفسه. هنا نفرق بين أمرين: الأول ، إذا كان المتهم أمينا على المال، عندئذ تقع جريمة خيانة الأمانة، والثاني ، إذا لم يتحقق شرط التسليم بوصف الأمانة ، فإن الأمر لا يسري عليه وصف التجريم. تطبيقا للفكرة الأخيرة قُضي ببراءة المتهم الذي استولى على مبلغ مالي أُودع في حسابه بالبنك بطريق الخطأ ، على سند من القول بأن الأمر يتعلق بمخالفة التزام تعاقدي[2]. وبالمثل فإن الزوج الذي يحوز أموالا مشتركة مع زوجته لا يرتكب جريمة السرقة إذا استولى لنفسه على مال مملوك لهما على الشيوع[3].

أما المعلومات المنسوخة ، فإنها تبقى في مكانها بعد عملية النسخ ، أي تبقى في حيازة صاحبها . للتغلب على هذه الصعوبة القانونية أقام القضاء الفرنسي نظريته في تحديد مفهوم اختلاس المعلومات.

٣٣- الاستعانة بفكرة الاختلاس المؤقت:

للتغلب على هذه الصعوبة لجأت أحكام القضاء الفرنسي إلى فكرة الاختلاس المؤقت[4]. واستعانت هذه الأحكام بمفهوم سبق أن لجأت إليه لاعتبار استعمال سيارة بدون إذن صاحبها فترة من الزمن وتركها في مكان غير معلوم من قبيل جريمة السرقة. هذا المفهوم هو اعتبار الاختلاس واقعا بالظهور على الشيء بمظهر المالك، وذلك حتى ولو كان لفترة مؤقتة.

---

(١) نقض ١٢ مايو سنة ١٩٥٢ مجموعة أحكام محكمة النقض س ٣ رقم ٣٤١ ص ٩١٥ ؛ ٢٥ ديسمبر سنة ١٩٥٦ ، س ٧ رقم ٣٦٣ ص ١٣٢ .

(2)Crim. 24 november 1983, D. 1984, 465 .

(3) Trib corr. Auxerre , 10 décember 1963, G.P. 1964, I, 185, D.1964 , Somm., 57.

(4) Crim. 12 janv. 1989, Bull. crim. n° 14, Rev. sc. crim. 1990. 346, et p. 507.

فقد أدرك القضاء الفرنسي أن من يقوم بنسخ المعلومات بدون موافقة صاحبها يظهر على الشيء المسجلة عليه المعلومة مظهر المالك، وقد يكون هذا الشيء هو جهاز الكمبيوتر أو الشريط أو الاسطوانة[١]. ويتجلى هذا الظهور في اغتصاب سلطة من سلطات المالك وهي نسخ المعلومة[٢]. ذلك أن هذا النسخ يجعل المعلومة غير مملوكة فقط لصاحبها، الذي أصبح يشاطره فيها الغير. وبالتالي انتهت أحكام القضاء إلى أن الاختلاس يقع بالظهور على الشيء بمظهر المالك[٣].

ومؤدى ما سبق أن الاختلاس – وفقا لما انتهت إليه أحكام النقض الفرنسي – يرد على المستند الأصلي، ولا يرد على الصورة الضوئية للمستند[٤] . وإذا تعلق الأمر بنسخ شريط أو اسطوانة أو نسخ معلومة من جهاز الكمبيوتر، فإن الشيء محل السرقة هو تلك الدعامة المادية من شريط أو اسطوانة أو الجهاز نفسه[٥]. هذا الاختلاس يتم بشكل مؤقت في أثناء الوقت اللازم لعملية النسخ[٦].

والقضاء الفرنسي إذ اجتهد في إبراز فكرة جديدة في الاختلاس وهي الظهور على الشيء بمظهر المالك، لم يتح له من حل مشكلة قانونية أخرى وهي أن هذا الاختلاس يحدث في وقت محدد للغاية وهو وقت يقوم فيه المتهم

---

(1) Reynald OTTENHOF, Infractions contre les biens, Rev.sc.crim. 1996,chronique de jurisprudence, p.863.

(٢) د. علي عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونيا " بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، كلية والشريعة والقانون ، دولة الإمارات ، المرجع السابق ص ٣٠ .

(3) Bouzat , Infractions contre les biens , Rev. sc. crim. 1987, chronique de jurisprrudence , p.211.

(4) Crim 1er janv. 1994, Dr. pénal , comm. 109.

(٥) انظر

Bouzat , op. cit. , p. 210 .

(6) Michel – Laure Rassat, Droit pénal spécial, Dalloz, 1997, p.73 .

بنسخ المعلومة. وهنا اعتد القضاء بفكرة الاختلاس المؤقت في أثناء الوقت اللازم للنسخ ، وذلك بالظهور على المعلومة المسجلة بمظهر المالك[1] .

٣٤- النتائج المترتبة على نظرية اختلاس المعلومات:

يترتب على إعمال نظرية الاختلاس المؤقت في خصوص جرائم الأموال، وخاصة في جريمة السرقة ، النتائج القانونية الآتية :

١- وقوع جرائم الأموال بتصوير المستندات:

٣٥-القول بأن المعلومات لها صفة المنقول يؤدي بنا إلى القول بوقوع جرائم الأموال (السرقة – النصب – خيانة الأمانة) إذا قام المتهم بتصوير مستند هام ينتمي إلى المجني عليه وحصل بذلك على صورة للمستند الأصلي ، تاركا إياه دونِ الاستئثار به . فما حصل عليه المتهم في هذه الحالة هو صورة للمستند أي للمعلومات الموجودة داخل المستند الأصلي، لكي يتمسك بها عند الضرورة [2]. ذلك ما حدث بالفعل في إحدى القضايا التي عرضت على محكمة النقض الفرنسية، حيث قام أحد العاملين الذي استغنت عنه إحدى الشركات بالدخول إلى مقر تلك الشركة وتصوير أحد المستندات لكي يقدمه إلى المحكمة المدنية التي رُفعت أمامها دعوى تعويض من جانب هذا العامل لفصله بطريق تعسفي كما يدعي. وقد احتج العامل بهذا المستند الذي يثبت أن الشركة ليست في وضع مالي سيئ يبرر الاستغناء عن عمله فيها. فقد انتهى القضاء الفرنسي إلى وقوع جريمة السرقة في هذه الحالة[3].

---

(1) Marie- Paule LUCAD DE LEYSSAC, op. cit. , p.47.
(2) Michel Veron, Droit pénal spécial, Armond Colin , 1999, p. 197.
(3) Arrêt Logabax , Crim, 8 janv. 1979 , D. 1979. 509; D. 1979. I.R. 182, Gaz. Pal.1979.2.501 ., crim. 29 av. 1986, D. 1987. 131, Rev. sc.crim., 1987. 701 , Crim. 24 oct. 1990, Bull. n° 355, Crim. 1994, Rev.sc.crim 1994, p. 767.

ويمكن أن نحاول تفسير ذلك الحكم بناء على القواعد العامة استنادا إلى أن المسروق هنا ليست المعلومات ولكنه المستند الذي قام المتهم بتصويره. فهو من لحظة تصويره يصبح ملكا لصاحب المستند الأصلي مادام قد تم تصويره في الشركة. فلا يجوز عندئذ أن يخرج إلاّ بإذن صاحب الشركة وإلاّ وقعت جريمة السرقة. ولكن ما القول لو أن المتهم قام بتصوير هذا المستند خارج مقر الشركة وبغير أوراقها أو أدواتها (ماكينة تصوير الشركة) . يُرد على ذلك بالقول بأن المستند الأصلي يكون قد تمت سرقته بشكل مؤقت في أثناء الوقت اللازم لتصوير المستند ، على غرار من قضت به المحاكم الفرنسية من وقوع جريمة سرقة السيارة باستعمالها بدون إذن صاحبها .

ويمكن تكملة حجج الرأي السابق بالقول بأنه لا مبرر للتمييز بين تصوير المستند داخل مكان وجوده وتصويره في خارج مكانَ وجوده ، وبأن محل السرقة في الحالتين هو المستند الأصلي الذي يظهر عليه المتهم بمظهر المالك . وبالتالي فإن السرقة تقع في أثناء الوقت اللازم لتصويره. ومادام القضاء الفرنسي قد سمح بوقوع السرقة على السيارة باستعمالها بدون رضاء صاحبها وذلك استنادا إلى الظهور عليها بمظهر المالك، فإن نظرية الاختلاس المؤقت تصبح مقبولة من الوجهة القانونية (1).

من الواضح أن المحاولة السابقة في التفسير ترمي إلى إعمال القواعد العامة في تحديد مفهوم المنقول وذلك بنفي هذه الصفة عن المعلومات البحتة غير المسجلة على دعامة مادية. بيد أن تلك المحاولة تصطدم بالقواعد العامة رغم ذلك ، عندما تنتهي إلى وقوع السرقة المؤقتة . وهي بذلك تستغني عن

(1) Bouzat, Infractions contre les biens , Rev .sc. crim. 1993 , chronique de jurisprudence , p. 546.

القصد الجنائي الذي يقوم على سند من نية التملك. ومن الواضح في هذا المثال أن نية تملك المستند الأصلي لا تقوم في هذه الحالة ، وأن نية الرد تتوافر ولا ريب في ذلك . كما أن المستند ليس من الأشياء التي تهلك مثل النقود والتي يعتبر استعمالها تصرفا فيها مفصحا عن توافر نية التملك . يضاف إلى ذلك أن السرقة ليست اعتداء على الملكية فقط ، بل إنها اعتداء أيضا على الحيازة. وذلك لا يتحقق في صورة تصوير المستند ، وخاصة عند القيام بذلك التصوير في نفس المكان الذي يوجد فيه المستند. أما الاحتجاج بالحكم الذي قضى بوقوع السرقة على السيار باستعمالها دون رضاء صاحبها ، فإنه قياس مع الفارق نظرا لاختلاف ظروف كل من الحكمين. ففي حالة السيارة يقوم المتهم بالاستيلاء عليها فترة من الزمن وتركها في مكان يصعب على صاحب السيارة معرفته ، معرضا إياها لخطر الضياع أو الهلاك . فما يهم المتهم هو الاستفادة بالسيارة في مدة معينة غير عابىء بحق صاحبها في ملكيتها، غير حريص على ردها إليه. هذه المعاني لا تتوافر في حالة تصوير المستند في فترة وجيزة مع الحرص على تركه لصاحبه ، مع الاعتراف بحق صاحبه عليه وعدم اتجاه قصد الفاعل إلى حرمان صاحبه من ملكيته أو من حيازته. هذه الملكية وتلك الحيازة يبقيها المتهم لصاحب هذا المستند الأصلي.

وبدلا من محاولة تطويع تصوير المستندات القواعد العامة في السرقة وذلك بمخالفة القواعد العامة من ناحية أخرى ، فإن اعتبار المعلومات البحتة أي غير المسجلة على دعامة مادية من الأموال المنقولة يساعد في حل تلك المشكلة القانونية ، وإن كان ذلك لا يتأتى دون صعوبة قانونية ، على نحو ما سبق أن أوضحناه.

وإذا كان وصف السرقة يثير بعض المشكلات القانونية بالنسبة

للمعلومات المبرمجة ، فإن وصف خيانة الأمانة أوضح في انطباقه إذا توافرت شروط تلك الجريمة ومنها شرط التسليم على وجه الأمانة لمعلومات مبرمجة على دعامة مادية (الجهاز – الشريط – الاسطوانة) . فالمادة ٣١٤ من قانون العقوبات المصري تجرم الاستعمال– بالإضافة إلى الاختلاس والتبديد – بوصفه نشاطا في جريمة السرقة . ويقصد بالاستعمال هنا ذلك الذي لا يصدر إلاّ من مالك[1]. ومن البين أن نسخ المعلومات المبرمجة هو من هذا القبيل[2].

٢–وقوع السرقة بنسخ المعلومات المبرمجة:

٣٦ -عُرض على القضاء الفرنسي مشكلة نسخ المعلومات المبرمجة ، سواء كانت مدونة على شريط أو اسطوانة أو كانت مسجلة داخل جهاز الكمبيوتر نفسه . وقد انتهت أحكام القضاء إلى اعتبار ذلك مشكلا لجريمة السرقة ، وذلك متى تم هذا النسخ على دعامة مادية . وبدأ الاعتراف شيئا فشيئا بالمعلومات المسجلة على دعامة مادية بوصفها من المنقولات . فقد قضت محكمة النقض الفرنسية بوقوع جريمة السرقة ممن قام بنسخ بعض أشرطة الكمبيوتر بدون رضاء صاحبها[3]. وعلى الرغم من أن المحكمة اعتبرت المتهم قد سرق النسخ الأصلية في أثناء الوقت اللازم لنسخها ، فإن الحكم يشير إلى أهمية المعلومات بصفتها من الأموال . كما أنه يثير مشكلات قانونية أكثر من تلك التي قام بحلها ، وهي مشكلة الاختلاس ومشكلة

---

(١) د. محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ،دار النهضة العربية ١٩٨٨ص١٢٠٦.

(2)Michel Margos, Michel Masse, Le droit pénal spécial né de l'informatique ,in " Travaux de l'institut de sciences criminelles de Poitiers, Informatique et droit pénal,", 1983, p. 31.

(3) Crim. 12 janv. 1989, Bull.crim. n° 14 (arêt Bourquin) ,Gaz Pal. 1989.2. somm. 283, Rev. sc.crim.1990.507.

السرقة الوقتية ومشكلة القصد الجنائي . وقد اتجهت أحكام للقضاء البلجيكي نفس الوجهة التي تبناها القضاء الفرنسي عندما اعتبر نسخ المعلومات مشكلا لجريمة السرقة [١] .

وبالنسبة لجريمة خيانة الأمانة ، فقد أصبح مستقرا في قضاء المحاكم الفرنسية أن قيام الأمين على الشريط بنسخه أو بإعطائه للغير لنسخة يتوفر به النشاط في الجريمة . فقد قضي بوقوع خيانة الأمانة من الأمين الذي أعطى أشرطة سينمائية لمسلسل تليفزيوني للغير ، لكي يقوم بنسخها إضرارا بصاحبها[٢] .

لذا فإن المحكمة ذاتها قضت بوقوع جريمة السرقة من العاملين في الشركة الذين استخدموا وثائق محاسبية خاصة بالشركة ، بدون رضاء صاحبها، لإعداد رسومات بيانية قاموا بتزويد الشركة المنافسة بها [٣] .

وقد لجأ القضاء للقول بصلاحية المعلومات المبرمجة للسرقة ، إلى تفسير مفهوم الاختلاس بأنه الظهور على الشيء بمظهر المالك . و لا يحول دون وقوع هذا الاختلاس – وفقا للأحكام القضاء – أن يتسم بالتأقيت ، أي أن يحدث في وقت محدد يقوم فيه المتهم بنسخ المعلومات .

هذا النسخ قد يتم من الجهاز نفسه أو من شريط أو من اسطوانة أو من ورقة . وقد يتم النسخ بنقل المعلومة إلى شريط أو اسطوانة أو إلى ورقة. فإذا كان ما قام به المتهم أنه نسخ معلومات تتعلق بأسماء العملاء الذين تتعامل معهم الشركة وقام باستخدام هذه المعلومات لتحقيق أغراض شخصية، فإن ذلك يكفي لوقوع جريمة السرقة وفقا لما قضت به محكمة النقض الفرنسة [٤].

---

(١) انظر :

Anvers , 13 déc. 1984 ; Corr. Bruxelles , 31 janv. 1986 ; Corr. Bruxelles 31 mai 1988 . مشار إليها في : Jean P. Spreutels , op. cit. , p.169 .

(2) Crim. 8 déc. 1971 , Bull.crim.,n° 341, p. 856.

(3) Crim . 1er mars 1989 , Bull. Crim. n° 100.

(4) Crim. 3 mars 1992, Bouzat , infractions contre les biens , chroniques , Rev. sc. crim. 1993, p.546.

وقد يتم النسخ بشكل مباشر باستعمال كمبيوتر الغير ، وقد يتم بالتداخل عن بعد في هذا النظام [1] .

ونظرا إلى أن اعتبار نسخ المعلومات المبرمجة مشكلا للسرقة يثير صعوبة قانونية في حالة إعمال القواعد العامة التقليدية ، فإن بعض التشريعات قد تضمنت نصا خاصا يجرم نسخ تلك المعومات بوصفه مشكلا لجريمة السرقة . من تلك التشريعات القانون النمساوي [2] .

٣٧ – مفهوم الاختلاس في القانون الإنجليزي لا يرتبط بالحيازة:

لا تعتبر السرقة في القانون الإنجليزي – على خلاف الوضع في القانون الفرنسي – اعتداء على الحيازة ، بل هي اعتداء على الملكية ، حتى ولو لم يقترن ذلك باعتداء على الحيازة، أي بخروج المال المسروق من حيازة المجني عليه إلى حيازة الجاني.

لذلك نص الفصل الثالث، فقرة أولى من " قانون السرقة " لسنة ١٩٦٨ على أنه: يعتبر اختلاسا كل اغتصاب لحقوق المالك، ويشمل ذلك ما يقوم به المتهم من احتفاظه لنفسه أو تعامله كمالك في مال دخل حيازته بطريق الخطأ أو التدليس [3].

---

(١) د. أحمد حسام طه تمام ، المرجع السابق ، ص ٤٥٧ .

(٢) انظر :

Peter J. Schick , Gabriele Schmölzer , Comoputer Crimes and Other Crimes against Information Technology in Austria, in " Délits informatiques et autres infractions à la technologie de l'information " , Rev. int. dr. pén. 1993, p. 156.

(3) Section 3 (1) of the Act provides : " Any assumption by a person of the rights of an owner amounts to an appropriation, and this includes ,where he has come by the property (innocently or not) without stealing it , any later assumption of a right to it by keeping or dealing with it as owner " .

الفرع الثالث

صعوبة القول بتوافر نية السرقة

٣٨ - نية التملك عنصر في القصد الجنائي في السرقة:

بالإضافة إلى الصعوبات السابقة ثارت صعوبة أخرى تتعلق بالقصد الجنائي في جريمة السرقة . ذلك أن القصد الجنائي لا يتوافر في حق المتهم بهذه الجريمة إلاّ إذا توافرت لديه نية السرقة . فبالإضافة إلى العلم بأن الشيء محل السرقة مملوك للغير فإن إرادة النتيجة عنصر من عناصر القصد الجنائي في جريمة السرقة . هذه الإرادة هي ما يعبر عنها القضاء والفقه بأنها نية التملك.

٣٨-تعريف نية التملك:

لا يتأتى ذلك إلاّ بتوافر نية حرمان المالك من سلطاته الفعلية كمالك وحلول المتهم محله في ممارسة هذه السلطات[١]. وتتحقق مظاهر هذه النية بقيام المتهم بممارسة السلطات التي لا تصدر إلاّ من مالك وهي سلطة الاستئثار بالشيء وسلطة التصرف. عندئذ يكون المتهم قد ظهر على الشيء بمظهر المالك وتجسدت لديه نية التملك[٢].

وتهتم أحكام القضاء بإثبات نية التملك باعتبار أن هذه النية تشكل قصد جنائيا خاصا[٣]. ويشايع كثير من الفقه هذا الاتجاه[٤]. لذا قُضي بنقض الحكم الذي اقتصر في أسبابه على تقرير أن المتهم استولى على مال مملوك للمجني عليه (قطع من الذهب) دون موافقة صاحبها ، وذلك في

---

(١) د. محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، ١٩٨٨، ص ٨٦٥.

(٢) د. محمود نجيب حسني ، المرجع السابق ، نفس الموضع .

(٣) د. محمود محمود مصطفى ، شرح قانون العقوبات – القسم الخاص ، دار النهضة العربية ١٩٨٤ ، ص ٤٨٠ ؛ د. محمود نجيب حسني ، المرجع السابق ، ص ٨٦٥ .

(٤) د. محمود نجيب حسني ، المرجع السابق ، نفس الموضع .

مقابل ما أداه هذا المتهم للمجني عليه من خدمات [1] . فقد نعت المحكمة على الحكم أنه يستظهر نية التملك ، ذلك أن الاستيلاء على المال قد يتم في هذه الحالة مع توافر نية الرد ، أي أن يكون ما استولى عليه المتهم على سبيل الرهن حتى يقوم المجني عليه بتسديد ما عليه من دين وبنية حرمان المجني عليه من ملكية المال محل النشاط . فالسرقة تقع اعتداء على الملكية بالإضافة إلى الحيازة وليس على الحيازة فقط . كما أنها تقع على الحيازة وليس على الملكية فقط .

٣٩- النتائج المترتبة على استلزام نية التملك:

يترتب على تخلف نية التملك نتيجة قانونية هامة تتمثل في انتفاء وصف السرقة عن بعض الأفعال ، وأهمها الاستعارة . ذلك أن استعارة الشيء يقترن بنية الرد ، الأمر الذي يتنافى مع نية التملك . فلا يعد سارقا – بسبب انتفاء نية التملك – "من يختلس صورة في غيبة صاحبها ليطلع عليها ويردها في الحال" [2] . وقد قضي بأن الجريمة لا تقع ممن يستولي على أدوات طباعة بقصد الاستعانة بها على طبع منشورات لسب مدير المطبعة والقذف في حقه ثم ردها لأن الاستيلاء بقصد الاستعمال المؤقت لا يكفي في القصد الجنائي [3]. كما قضي بعدم توافر نية التملك ممن أخذ شيئا من مدينه وأبقاه عنده كرهن له على دينه لأنه لا يمتلك الشيء ولم يحزه إلاّ حيازة مؤقتة ، بل ولم يستعمله [4].

٤٠- نية حرمان المجني عليه من المال المسروق أمر متطلب في القانون المقارن:

لا تقع جريمة السرقة إلا مع توافر نية التملك وفقا للقوانين المقارنة. وقد

---

(1) Crim 22 décembre 1955, B.C., n. 594.

(٢) د. محمود محمود مصطفى ، المرجع السابق ، ص ٤٨١.

(٣) نقض ١٨ أكتوبر سنة ١٩٤٣ ، مجموعة القواعد القانونية جـ ٦ رقم ٢٣٩ ص ٣١٦ .

(٤) بني سويف الجزئية ، ١٧ نوفمبر سنة ١٩٢٠ المحاماة س ١ رقم ١٢٠ ص ٥٤٤ ، مشار إليه في د. محمود نجيب حسني ، شرح قانون العقوبات – القسم الخاص ، المرجع السابق ص ٨٦٧

عبر القانون الفرنسي عن ذلك باستعماله – في المادة ٣١١ / ١ من قانون العقوبات – تعبير " من اختلس بسوء نية " frauduleusement [1] .

ويتطلب القانون الإنجليزي نية التملك أيضا ، وقد استعمل تعبير "بسوء نية" dishonestly " وتعبير" بنية حرمان صاحب المال نهائيا منه " with the intention of permanently depriving the other of it " ، للدلالة على ذلك بنصه في الفصل الأول من قانون السرقة لسنة ١٩٦٨ : " يعتبر الشخص مرتكبا للسرقة إذا استولى لنفسه ، بسوء نية ، على أموال تنتمي إلى الغير ، بنية حرمان هذا الأخير بشكل دائم منه "[2]. وبهذا فإن قانون السرقة في إنجلترا قد تبنى ما سبق أن استقر عليه القضاء الإنجليزي قبل صدور هذا القانون من أن الاستيلاء على مال الغير بنية حرمانه مؤقتا من ملكه لا يشكل جريمة السرقة كما هي معرفة به في السوابق القضائية[3].

وعلى الرغم من أن القانون الإنجليزي قد أرسى القاعدة العامة السابقة في تطلب نية حرمان المجني عليه نهائيا من ملكه ، فإنه قد أورد استثناء عليها في قانون السرقة لسنة ١٩٦٨ . فتنص الفصل ٦ من القانون سابق الذكر على حالتين تتوافر فيه نية السرقة خروجا على القاعدة السابقة ، وهما : ١ – إذا اتجهت نية المتهم إلى الظهور على الشيء بمظهر المالك ، متصرفا فيه إضرار بصاحب الحق فيه . ٢ – إذا استعار المتهم الشيء أو أعاره لمدة وفي

---

(1) Jean PRADEL , Michel DANTI- JUAN , Droit pénal spécial , éd. Cuja, 1995 ,p.550.00

(2) " (1) A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it ; and " thief " and "steal " shall be construed accordingly " .

(3) Warner (1970) 55 Cr. App. Rep. 93 .

ظروف تجعل هذا السلوك بمثابة استيلاء أو تصرفا في الشيء "[1].

ومن التطبيقات على الحالة الأولى التي بمقتضاها تتوافر نية السرقة على الرغم من توافر نية الرد ما قام به المتهم من الاستيلاء على مبلغ من النقود من حسابات العملاء دون موافقة صاحب الحق في ذلك ، معتبرا ذلك من قبيل القرض، أي منتويا رد هذا المبلغ بعد استثماره . فقد قُضي بارتكاب الجريمة – وفقا لقانون السرقة ١٩٨٦ – بانطباق الفقرة الأولى الاستثنائية سابقة الذكر – حيث قام المتهم بالظهور على الشيء بمظهر المالك ، متصرفا فيه إضرار بصاحب الحق فيه " قضية Fernandes ١٩٩٦ "[2]. ومؤدى ذلك أن استيلاء المتهم على ملك الغير في ظروف تدل على احتمال عجزه عن تحقيق ما انتواه من رد الشيء المسروق يدل على توافر قصد السرقة على الرغم من توافر نية الرد. ويستند الفقه الإنجليزي في ذلك إلى أن ذلك يعد من قبيل الظهور على الشيء بمظهر المالك[3].

وبالمثل فإن استعارة الشيء يمكن أن ترقى – في نظر القانون الإنجليزي – إلى السرقة على الرغم من توافر نية الرد إذا كانت الاستعارة لمدة طويلة . ويضرب الفقه مثلا على ذلك بوقوع الجريمة إذا استولى طالب على كتاب بدون وجه حق من المكتبة وتوافرت لديه نية رد هذا الكتاب عندما ينتهي

---

(1) Section 6 : " A person appropriating property belonging to another without meaning the other permanently to lose the thing itself is nevertheless to be regarded as having the intention of permanently depriving the other of it : (i) if his intention is to treat the thing as his own to dispose of regardless of the other's rights ; and (ii) a borrowing or lending of it may amount to so treating it if , but only if , the borrowing or lending is for a period and in circumstances making it equivalent to an outright taking or disposal " .

(2) Alan Reed, Peter Seago , Criminal law , ed. Sweet and Maxwell, 1999, p. 434 .

(3) Reed , Seago , id . , p. 435 .

من دراسته للمادة والتي تستمر سنوات عديدة بالكلية[1].

ومن التطبيقات على انتفاء الجريمة لتوافر نية الرد الفوري ما قضي به في إنجلترا بأن المتهم الذي يعمل في صالة عرض أفلام السينما والذي قام بتسليم أشرطة تسجيل بعض الأفلام إلى أصدقاء له ليقوموا بنسخها وإعادتها في الحال لا يتوافر لديه نية حرمان المجني عليه من ماله " قضية Llyod١٩٨٥ " وبالتالي قضي ببراءته من أي اتهام ينص عليه قانون السرقة لسنة ١٩٦٨ [2] .

وخلاصة ذلك أن نية الرد تكشف عن أن الأمر يتعلق باستعارة وليس بسرقة[3]. والاستعارة غير القانونية لا تعتبر – وفقا للقواعد العامة – من قبيل السرقة، إلاّ إذا اتجه قصد المتهم إلى إعادة الشيء إلى صاحبه بعد أن فقد قيمته[4].

٤١- ضرورة النص الخاص لتجريم استعمال النظام دون موافقة صاحبه :

تتجه تشريعات عديدة إلى تجريم سرقة وقت الكمبيوتر، بالمخالفة للقواعد العامة التي تنتهجها تلك التشريعات من عدم تجريم استعمال ملك الغير دون رضائه، وإعمالا للقواعد العامة في تشريعات أخرى تجرم استعمال ملك الغير دون رضائه[5]. أما الطائفة الأولى من التشريعات فإنها قد تبنت هذا النوع من التجريم على غرار ما اتبعته بالنسبة لتجريم استعمال سيارة ملك الغير بدون رضائه. فعلى الرغم من عدم توافر نية التملك ، فإن الفعل يشكل جريمة بنص خاص .

---

(1) Alan Reed, Peter Seago , id . , p.432.
(2) Reed , Seago, id , p. 433.
(3) J. C. Smith , The law of theft , seventh Ed. Butterworths, London, 1993 , p. 66 .
(4) Reed , Seago , id , p. 433 .

(٥) انظر سابقا رقم ٤٠ .

المطلب الثاني

الصعوبات القانونية المتعلقة بإعمال قواعد النصب

في مجال الكمبيوتر والإنترنت

٤٢- تثور مشكلات قانونية تتعلق بمدى انطباق أحكام النصب في مجال بعض الجرائم التي تقع بطريق الكمبيوتر . من هذه الصعوبات ما يتصل بالنشاط في النصب وهو الاحتيال ، ومنها ما يتصل بالنتيجة وهي تسليم الأموال.

الفرع الأول

مدى وقوع الاحتيال بالكمبيوتر وعلى الكمبيوتر

٤٣- قد تقع جريمة النصب بالاستعانة بالكمبيوتر لإتمامها ، وقد تقع على نظام الكمبيوتر نفسه ، بل إن هذه الجريمة قد تقع من المتهم مستعينا بالكمبيوتر وذلك بالنصب على نظام كمبيوتر آخر .

وقد ثارت مشكلة قانونية تتعلق بمدى جواز الاحتيال على الكمبيوتر أو على الآلة بوجه عام . ذلك أنه من المألوف أن جريمة النصب تقع على الإنسان.

٤٤- الأصل أن النصب يقع على الإنسان:

الأصل أن المجني عليه في النصب هو إنسان يُخدع بوسيلة احتيالية . فتنص المادة ٣٣٦ من قانون العقوبات على أنه "يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو أي متاع منقول وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها إما

باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطرق الاحتيال أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور .... " .

يتضح من النص السابق أن المشرع استعمل تعبير " إيهام الناس " في إشارة إلى المجني عليه في جريمة النصب . ومادامت جريمة النصب تقع اعتداء على رضاء المجني عليه بالإضافة إلى وقوعها اعتداء على ملكيته ، فإن هذا الرضاء هو من سمات الإنسان وليس من سمات الآلة. والحقيقة أن الإنسان هو الذي يقع في غلط أو يقع تحت تأثير التدليس في العقود وفقا لقواعد القانون المدني أيضا ، ذلك أن الذي يتعاقد هو إنسان سواء كان يعمل لصالح شخص طبيعي أو لحساب شخص معنوي.

٤٥- الآلة تحل محل الإنسان كمجني عليه :

مع ازدياد استعمال الآلة في التعامل مع الجمهور بدأت مشكلات قانونية تُثار حول تأثير هذا الحلول على المسئولية الجنائية للمتعامل مع الآلة وكذلك صاحب الآلة نفسها.

فهناك أولا حلول الآلة محل صاحبها. هذا الحلول لا يعفيه من المسئولية بوصف الخطأ عندما تقع جريمة تسبب استعمال الآلة في حدوثها ،مادام صاحبها لم يكن منتويا استعمالها. في هذه الحالة تنتفي المسئولية الجنائية للمتهم إذا لم يكن القانون يعاقب عليها بوصف الخطأ . وعلى العكس من ذلك إذا كان تسبب المتهم عمدا أن تؤدي الآلة نتيجة معينة كتفجير شحنة ديناميت ، فإن مسئوليته الجنائية بوصف العمد تنعقد عن فعل الآلة . ذلك

أنه من المقرر أن استعمال المتهم آلة معينة لا ينفي عنه صفة الفاعل الأصلي في الجريمة. كذلك قد يستعمل المتهم واسطة لا إرادة لها كحيوان أو طفل صغير. وذلك لا ينفي عنه أنه هو الذي قام بالنشاط . وبالمثل فإن استعماله للآلة كالكمبيوتر لا ينفي عنه صفة الفاعل الأصلي في الجريمة.

ولا نخال أن الوضع القانوني يختلف بالنسبة للشخص المتعامل مع الآلة بدلا من الإنسان. فإذا أوقع المتهم الآلة في غلط باستعمال وسيلة احتيالية ، فإن لا شيء يحول دون اعتبار ذلك مشكلا لجريمة النصب. لذا قضت محكمة النقض الفرنسية بوقوع جريمة النصب من المتهم الذي استعمل عملة لا قيمة لها واضعا إياها في عداد موقف السيارات فتحصل بذلك على إعفاء من التزامه بدفع مبلغ انتظار سيارته مدة معينة في هذا الموقف[1]. ولم تتبن المحكمة ما يراه البعض من أن وضع قطعة معدنية عديمة القيمة في آلة توزيع المشروبات يشكل جريمة السرقة على غرار استعمال مفتاح مصطنع في فتح تلك الآلة [2]. كما لا يتمشى هذا القضاء مع ما قُضي به في بلجيكا من وقوع جريمة السرقة ممن توصل إلى سحب مبلغ مالي من آله التوزيع النقدي بالبنك باستعمال كارت سحب مزور أو مسروق باعتبار أن استعمال كارت السحب من قبيل استعمال مفاتيح مصطنعة[3]. والحق أن المتهم لم يفتح الآلة. لذلك نحن ننضم إلى الحكم الذي اعتبر استعمال تلك الوسيلة بمثابة استعمال لطرق احتيالية في جريمة النصب.

---

(1) Crim. 10 déc. 1970 , J.C.P. 1972.II.17277, D. 1972, p. 155 .

(٢) د. محمود نجيب حسني ، شرح قانون العقوبات - القسم الخاص ، دار النهضة العربية ١٩٨٨ ص ٨٥٣.

(٣) انظر أحكام للقضاء البلجيكي :

Corr. Liège 22 mars 1982,; Bruxelles 22 mars 1973 ،

مشار إليها في : Jean P. Spreutels , Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Belgique , in " Délits informatique et autres infractions à la technologie de l'information " , Rev. int. dr. pén. 1993, p. 163

٤٦- وقوع النصب على الآلة:

تستعمل كثير من البنوك آلات للسحب الآلي لكي يتعامل معها الجمهور فتسمح لهم بالحصول على مبالغ مالية من حسابهم . هذه الآلات هي في الحقيقة نظام للكمبيوتر متصل بحسابات العملاء .

يظهر العرض السابق أن لا شيء يحول دون وقوع الاحتيال على الكمبيوتر وبالتالي وقوع جريمة النصب بالاستيلاء على مال منقول مملوك للغير بناء على هذا الاحتيال.

إلى تلك النتيجة انتهى القضاء الكويتي، حيث ذهب في أحد أحكامه إلى وقوع جريمة النصب من المتهمة التي استولت على كارت السحب الآلي للمجني عليه بالإضافة إلى رقمه السري وقامت بسحب مبلغ مالي من حساب صاحب هذا الكارت. فقد اعتبرت محكمة التمييز الكويتية أن ما قامت به المتهمة انتحال لصفة غير صحيحة وهي أنها صاحبة الحساب أو أنه وكيل عن صاحب هذا الحساب . لذا قضت المحكمة بوقوع جريمة النصب تامة في هذه الحالة ، وذلك بسحب المبلغ المالي من حساب المجني عليه . وقد أبانت المحكمة رأيها بقولها إن "انتحال المتهمة صفة غير صحيحة بأنها صاحبة الحق في السحب من حسابي المجني عليهما في حمل كل من البنكين على تسليمها المال عن طريق جهازه الآلي يكفي وحده في تكوين ركن الاحتيال ولو لم يكن فيه استعمال لأساليب الغش والخداع المعبر عنها في المادة ٢٣١ من قانون الجزاء بالطرق الاحتيالية وهو ما يوفر في حقه جريمة النصب المرفوعة بها الدعوى لا السرقة ، لأن تسليم المال إليها تمّ بالرضاء ولو عن غلط ، وهذا الرضاء يعد نافيا للاختلاس الذي يفترض فيه استيلاء الجاني على المال دون رضاء المجني عليه "[1].

---

(١) تمييز ٢٨ / ٥ / ٩٠ طعن رقم ٢٤٢ / ٨٩ جزائي ، مجموعة القواعد القانونية التي قررتها محكمة التمييز خلال الفترة من ١/١/٩٦ ، ص ٦٩٢ .

أما إذا اقتصر سلوك المتهم على استعمال كارت صحيح للسحب الآلي ولكنه سحب من رصيده أكثر مما يسمح به ذلك الرصيد ، فإن القضاء الفرنسي انتهى إلى انتفاء وصف التهمة عن هذا الفعل ، واقتصار الأمر على مخالفة التزام تعاقدي[1].

وقد أعمل القضاء الفرنسي فكرة النصب على الكمبيوتر عندما قضى بتوافر تلك الجريمة من المتهم الذي أعطى أمرا إلى الكمبيوتر بتحويل مبالغ نقدية من الشركة التي يعمل بها لحساب شركة أخرى يسيطر عليها ، وذلك للاستيلاء عليها لنفسه[2]. فقد استقر القضاء الفرنسي على وقوع جريمة النصب إذا سحب المتهم مبالغ نقدية من حساب شخص غيره باستخدام كارت السحب الآلي لهذا الشخص أو إذا قام بتسديد ثمن مشترياته باستعمال كارت الغير[3].

وإذا كان الاحتيال على الكمبيوتر قد يتوافر بفعل من المتهم الذي يستعمل كارت السحب، فإنه ليس هناك ما يحول دون الاستعانة بجهاز كمبيوتر للاحتيال على كمبيوتر آخر. فقد يتوصل المتهم إلى معرفة كلمة السر، أو رقم سري للدخول إلى نظام كمبيوتر خاص بأحد البنوك أو بإحدى الشركات، فيقوم باستعماله في إعطاء أمر لهذا النظام الأخير لتحويل مبلغ نقدي إلى حساب خاص به أو بأحد معارفه . فلا شيء يحول دون إضفاء وصف النصب على هذا الفعل[4].

---

(١) انظر

Crim. 24 nov. 1983, D.1984, 465.

(2) Trib. correc. De Thionville , 3 juin 1997 , Expertises, n° 208, oct. 1997, p. 317. obs Bertrand.

(٣) انظر

Bordeaux 25 mars 1987 , D. 87 , juris. p. 424, p Paris 11 fév. 1988 cité par Vasseur , D. 82. I . R. , p. 500 .

(٤) د. أحمد حسام طه تمام ، المرجع السابق ، ص ٥١٠ .

فإذا عمد المتهم إلى استعمال طريق Salami التي تتمثل في إعطاء أمر إلى الكمبيوتر لتحويل المبالغ النقدية البسيطة في الحسابات المختلفة للعملاء إلى حسابه الخاص حتى يتم ذلك بطريقة غير ملحوظة بسبب صغر المبالغ المحولة ، فإن ذلك يصح اعتباره من الحيلة التي تنطلي على الجهاز. فالأمر هنا هو برنامج يهدف إلى خداع الكمبيوتر. فإذا ما تمّ ذلك ونفذ الجهاز ذلك البرنامج فإنه يكون قد وقع في غلط بسبب إدخال هذا البرنامج على أنه برنامج صحيح صادر من صاحب الحق في إعطائه. فالبرنامج هو إذن من الوسائل الإحتيالية – في رأينا – والتي يتوافر بها النشاط في جريمة النصب.

والقول بوقوع النصب على الآلة يتفق مع المعمول به في بلاد عديدة مثل فرنسا وهولندا وكندا وعدة قوانين في الولايات المتحدة الأمريكية [١] . ولكن التفسير القضائي في قوانين أخرى كثيرة يستبعد وقوع النصب على الآلة ومن ثمّ يستبعد وقوع جريمة النصب على الكمبيوتر[٢]. من هذه القوانين قانون العقوبات في النمسا [٣] والدانمارك [٤] وفنلندا وألمانيا واليونان[٥] وإيطاليا [٦] واليابان [٧] ولكسمبورج [٨] والنرويج والسويد [٩] وسويسرا[١٠] . وتطرد أحكام القضاء الإنجليزي على أن النصب لا يكون إلاّ عقل بشري ، وبالتالي فإن جريمة النصب لا تقع إذا كان الاحتيال موجها إلى

---

(١) انظر section٤٩٦ من القانون البلجيكي و sections٣٣٨, ٣٨٧ and٣٣٨ من القانون الكندي و section٣٢٦ من القانون الهولندي .

(٢) انظر

Ultrich Sieber, id, at 41 .

(٣) انظر section١٤٦ من قانون العقوبات النمساوي

(٤) انظر section٢٧٩ من قانون العقوبات الدانمركي

(٥) انظر section٣٨٦ من قانون العقوبات اليوناني

(٦) انظر section٦٤٠ من قانون العقوبات الإيطالي

(٧) انظر section٢٤٦ من قانون العقوبات الياباني

(٨) انظر section٤٩٦ من قانون العقوبات في لكسمبورج

(٩) انظر Chapter٩, section ١ من قانون العقوبات السويدي

(١٠) انظر section١٤ من القانون السويسري .

جهاز للكمبيوتر[1].

٤٧- تجريم النصب بطريق الكمبيوتر بنص خاص:

نظرا لما يُثار من مشكلات قانونية تتعلق بالاحتيال بطريق الكمبيوتر، تفضل بعض التشريعات تجريم النصب بطريق الكمبيوتر بنص خاص. وبناء عليه يعتبر استعمال الكمبيوتر أو التدخل في نظام الكمبيوتر والحصول على فائدة مادية من قبيل الجريمة المعاقب عليها بنص خاص. من تلك التشريعات قانون العقوبات الياباني (في المادة ٢٤٦/ ٢ منه) الذي يعاقب على الاستعانة بمعلومات مبرمجة كاذبة أو إدخال هذا النوع من المعلومات في نظام كمبيوتر لشخص آخر للحصول لنفسه أو للغير على ربح غير مشروع [2].

(١) أنظر
Re London and Globe Finance Corp. (1903) 1 Ch. 728 ; DPP v Ray (1973).
مشار إليه في : Martin Wasik , Computer Crimes and Other Crimes against Information Technology in the United Kingdom , Rev.int.dr.pén.1993,p.643.
(٢) انظر :
Atsushi Yamaguchi, Computer Crimes and Other Crimes against Information Technology in Japan , Rev.int.dr.pé .1993, op.cit.

الفرع الثاني

جواز التسليم الرمزي في جريمة النصب

٤٨ – يشكل التسليم عنصرا في الركن المادي في جريمة النصب. هذه الجريمة لا تكتمل إلاّ بتحقق هذا التسليم . قبل ذلك يمكن أن يعد الفعل مشكلا للشروع في نصب. هذا الشروع تعاقب عليه المادة ٣٣٦ من قانون العقوبات " أما من شرع في النصب ولم يتممه فيعاقب بالحبس مدة لا تتجاوز سنة ".

وقد يتخذ التسليم شكل التسليم الحقيقي ، وقد يكون تسليما رمزيا. وقصد بالتسليم الحقيقي المناولة المادية للشيء محل النصب. أما التسليم الرمزي ، فإنه يتحقق بتسليم ما يرمز إلى الشيء الحقيقي . فتسليم سند الملكية يرمز إلى تسليم البضاعة التي يثبتها هذا السند.

ويتصل بمشكلة التسليم الرمزي أن يتم التسليم عن طريق قيد مبلغ مالي في حساب المتهم عن طريق الكمبيوتر[١]. فلا شيء يتنافر مع القواعد العامة إذا اعتبرنا أن ذلك يتحقق به عنصر النتيجة في جريمة النصب [٢] . تطبيقا لذلك قضت محكمة النقض الفرنسية بوقوع جريمة النصب تامة بتسجيل مبلغ نقدي في حساب المتهم ، حتى ولو لم يقم بصرف هذا المبلغ . وانطلاقا من نفس الفكرة فإن التسليم الرمزي يتحقق إذا خُصم من حساب شخص لدى البنك مبلغٌ ماليٌّ معينٌ من دين الضرائب عليه ، وكان هذا الخصم ناتجا عن استعمال وسائل احتيالية في مواجهة إدارات معينة بوزارة المالية تمكن المتهم من إقناع الموظفين بها أنه يستحق هذا الخصم [٣]. ومؤدى ذلك أن المتهمُ يسأل عن الجريمة تامة وليس عن الشروع في جريمة في هذه الحالة .

---

(١) انظر

Guillaume CHAMPY, La fraude informatique , Presses Universitaires d'Aix - Marseille , 1992, p. 52

(2) Michel MARGOS, Michel MASSE, " Le droit pénal spécial né de l'informatique , in " Informatique et droit pénal ", Travaux de l'institut de sciences criminelles de Poitiers, éd. Cujas, 1983, p. 29 .

(3) Vouin et Rassat, Droit pénal spécial , 4 eme éd. p. 65 .

المبحث الثالث

مدى اعتبار المعلومات المبرمجة محررات

يحميها قانون العقوبات

٤٩ - المقصود بالمحرر:

لم تضع المادة ٢١١ وما يليها من قانون العقوبات مصري تعريفا للمحرر في مفهوم جرائم تزوير المحررات . واكتفت المادة ٢١١ عقوبات بالعقاب على التزوير في " أحكام صادرة أو تقارير أو محاضر أو وثائق أو سجلات أو دفاتر أو غيرها من السندات والأوراق الأميرية ... " . كما تعاقب المادة ٢١٢ عقوبات مصري على التزوير في أو أوراق عرفية دون الإشارة إلى محل التزوير. أما المادة ٢١٣ عقوبات فإنها قد استخدمت – في صدد عقابها على التزوير في أوراق رسمية بطريق التزوير المعنوي – تعبير "السندات " في معالجتها لذلك النوع من التزوير . بينما فضل المشرع – في المادة ٢١٤ عقوبات عند تجريم استعمال المحررات المزورة – استعمال تعبير " الأوراق المزورة ".

وقد اكتفى قانون الجزاء الكويتي ، باستعمال تعبير " المحرر" دون إيراد تعريف له أو إعطاء أمثله لصور منه . فتنص المادة (٢٥٧) جزاء على أنه " يُعد تزويرا كل تغيير للحقيقة في محرر بقصد استعماله .... " . أما المشرع في دولة الإمارات العربية المتحدة فقد استعمل تعبير "المحررات" عند معالجة جرائم التزوير في الفرع الثاني الذي جاء عنوانه "تزوير المحررات " والذي جاء منتميا إلى الفصل الخامس . هذا الفصل الأخير ينتمي إلى الباب الأول من الكتاب الثاني. وجاء عنوان هذا الباب الأول "الجرائم الماسة

بأمن الدولة ومصالحها " . وقد استعمل قانون العقوبات الاتحادي تعبير " المحرر " في كل مرة عالج فيها جريمة التزوير ، سواء في صدد تعريفه للتزوير بوجه عام (مادة ٢١٦ عقوبات) أو في تجريمه للتزوير في أوراق رسمية أو للتزوير في أوراق عرفية أو لاستعمال المحررات مزورة . ومع ذلك يلاحظ أن الفقرة (٥) من المادة ٢١٦ عقوبات اتحادي استعملت تعبير " الأوراق " وليس المحررات بقولها " ملء ورقة ممضاة أو مختومة أو مبصومة على بياض ... " .

وبحثا في قانون الإثبات في المواد المدنية والتجارية المصري رقم ٢٥ لسنة ١٩٦٨ ، نجد أنه لم يبين في صدد تعريفه للمحرر الرسمي والمحرر العرفي طبيعة المحرر وما إذا كان يمكن إدراج البيانات المبرمجة ضمنها . فقد عرفت المادة (١٠) منه المحررات الرسمية بأنها " هي التي يثبت فيها موظف عام أو شخص مكلف بخدمة عامة ما تمّ على يديه أو ما تلقاه من ذوي الشأن وذلك طبقا للأوضاع القانونية وفي حدود سلطته واختصاصه " . كما عرفت المادة (١٤) المحرر العرفي بقولها " يعتبر المحرر العرفي صادرا ممن وقعه ما لم ينكر صراحة ما هو منسوب إليه من خط وإمضاء أو ختم أو بصمة .... " .

وقد جاءت صياغة قانون الإثبات في المعاملات المدنية والتجارية (قانون اتحادي رقم (١٠) لسنة ١٩٩٢ على غرار قانون الإثبات في مصر . فتنص المادة ٧/ ١ منه على أن "المحررات الرسمية هي التي يثبت فيها موظف عام أو شخص مكلف عامة، ما تم على يديه أو ما تلقاه من ذوي الشأن وذلك طبقا للأوضاع القانونية وفي حدود سلطته واختصاصه " . وفي خصوص المحرر العرفي حددت الفقرة الثانية من المادة ذاتها مفهومه بقولها "

فإذا لم تكسب هذه المحررات صفة رسمية فلا يكون لها إلاّ قيمة المحررات العرفية متى كان ذوو الشأن قد وّقعوها بإمضاءاتهم أو بأختامهم أو ببصمات أصابعهم ".

وعلى الرغم من عدم تضمن قانون العقوبات المصري تعريفا للتزوير ، فإن الفقه يعرّفه بأنه " تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر ومقترن بنية استعمال المحرر المزور فيما أعد له "[١].

وبناء عليه يمكن تعريف المحرر بأنه مستند مكتوب منسوب صدوره إلى شخص أو إلى جهة يصلح للاحتجاج به لترتيب أثار قانونية .

٥٠- المعلومات المبرمجة لا تنتمي إلى المحررات:

تثير المعلومات المبرمجة في جهاز الكمبيوتر أو على اسطوانة أو شريط مشكلة قانونية من حيث انطباق وصف المحرر عليها وبالتالي وصف جريمة التزوير[٢]. ذلك أن المحرر الذي يحميه تجريم التزوير هو ذلك الذي يصلح للاحتجاج به. وموطن الحماية في المحرر هو البيان الجوهري الذي يولد عقيدة مخالفة لدى المطلع عليه ، الأمر الذي يفترض أن المحرر يتم استعماله في التعامل. وهذا لا يتحقق بالنسبة للمعلومات المبرمجة قبل أن تتم طباعتها في أوراق . فالمصلحة محل الحماية في جرائم التزوير هي الثقة العامة [٣] . لذا

(١) د. محمود نجيب حسني ، " شرح قانون العقوبات – القسم الخاص " ، دار النهضة العربية، ١٩٨٨ص ٢١٤ .

(2) Travaux de l'Institut de sciences criminelles de Poitiers, Informatique et droit pénal , éd. Cujas , 1983 , p. 30 .

(٣) د. أحمد شوقي الشلقاني ، الضرر في تزوير المحررات ، رسالة ، جامعة القاهرة ، ١٩٨٠ ص ١٩٨.

فضل المشرع المصري استعمال تعبير "مستندات". فالمعنى المألوف للمحرر هو إذن الأوراق [١].

ويرجع السبب في صعوبة اعتبار المعلومات المبرمجة من قبيل المحررات إلى اشتراط أن تكون الكتابة المدونة بالمحرر ظاهرة يمكن قراءتها [٢] . لذا عبر رأي في الفقه عن ذلك بتعريفه المحرر بأنه " مسطور يتضمن علامات ينتقل بها الفكر لدى النظر إليها من شخص إلى آخر " [٣] . وعلى الرغم من أنه لا عبرة بالمادة التي كتب عليها المحرر ، فقد تكون من الورق أو الحجر أو الخشب أو القماش أو الجلد أو غير ذلك [٤] ، فإنه من اللازم أن تكون هناك كتابة ظاهرة يبرزها المحرر [٥] [٦] . كما أنه يلزم في المحرر أن يكون معدا لتقديمه للغير للتمسك به عند اللزوم . لذا اتجه الرأي إلى عدم انطباق وصف المحرر على المعلومات وإن كانت مبرمجة على دعامة مادية وبالتالي استبعد وصف التزوير عنها[٧]. وإلى هذه الوجهة اتجهت أحكام للقضاء الفرنسي[٨] وأحكام للقضاء في اليابان[٩].

---

(١) د. عمر الفاروق الحسيني ، المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، ١٩٩٥ص ٨٠.

(2) Vitu, Traité de droit pénal spécial , n° 1196 .

(٣) د. محمود محمود مصطفى ، شرح قانون العقوبات – القسم الخاص ، دار النهضة العربية ، ١٩٨٤ ص ١٤٢ .

(٤) د. محمود محمود مصطفى ، المرجع السابق ، ص ١٤٢ .

(٥) د. محمود نجيب حسني ، المرجع السابق ، ص ٢٤٧ .

(6) Vitu , Traité dr droit pénal spécial, n° 1196.

(7) Wilfrid JRANDIDIER, Interprétation de la loi pénale , Juris –class . pénal, Art 111 –2 à 111 – 5 , n° 38.

(٨) د. محمد سامي الشوا ، المرجع السابق ص ١٦ .

(٩) انظر :

Atsushi Yamaguchi, Computer Crimes and Other Crimes against Information Technology in Japan , Rev.int.dr.pén.1993, p. 437.

ومع ذلك فإن أحكاما للقضاء الياباني قضت باعتبار المعلومات في أجهزة كمبيوتر إدارة المرور من المحررات في مفهوم جريمة التزوير ، باعتبار أن لها حجة في الإثبات : انظر المرجع السابق ، نفس الموضع .

وقد انتهت أحكام للقضاء في دول مختلفة إلى إعمال وصف المحرر على الشرائط المغنطة ، إذا كانت حجة في الإثبات . من ذلك أحكام للقضاء الياباني [١] وأحكام للقضاء السويسري [٢] .

بيد أن ذلك ليس محلا لإجماع الفقه . فهناك من لا يرى سببا لاستبعاد المعلومات المبرمجة من عداد المحررات مادامت مدونة على اسطوانة أو شريط أو مسجلة بجهاز الكمبيوتر نفسه ، استنادا إلى أنه يمكن قراءتها بالأسلوب الخاص بها . فليس هناك ما يستوجب أن يكون المستند قابلا للقراءة بالعين المجردة [٣] . وقد صدرت من القضاء الفرنسي [٤] وكذلك من القضاء الهولندي [٥] ومن القضاء الإسرائيلي [٦] أحكام أعملت فيها أحكام التزوير في خصوص المعلومات المبرمجة في بعض الحالات التي تصلح فيها حجة للتمسك بها .

بيد أن ما يضعف حجج المنادين باعتبار بالبيانات المبرمجة من قبيل

---

(١) قضت أحكام للقضاء الياباني باعتبار المعلومات في أجهزة كمبيوتر الخاصة ببعض الإدارات مثل إدارة المرور من المحررات في مفهوم جريمة التزوير ، باعتبار أن لها حجة في الإثبات : انظر ، Atsushi Yamaguchi نفس الموضع .

(٢) انظر

Robert Roth , Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatiques en Suiss, Rev.int.dr.pén.1993,p.595.

(3) Smith & Hogan, Criminal law , cases and materials ,Third edition Butterworths, London , 1986, p. 517.

(٤) انظر

Corr. Paris , 12 oct. 1988 , J.C.P.1989 , II, 21253 .

(٥) انظر :

Appel La Haye , ٢٢mai ١٩٨٩ مشار إليه في :

Jean Spreutels , op. cit. , p. 167 .

(٦) انظر :

Eli Lederman , Computer Crimes and Other Crimes against Information Technology in Israel , Rev.int.dr.pén.1993,p.410.

المحـررات في مفهـوم التزويـر أن تلـك الجريمـة لا تقـع إلاّ إذا تـوافرت نيـة استعمال المحرر المزور فيما زُور من أجلـه . هـذه النيـة لا يمكـن أن تتواجـد بالنسبة للبيانات التي لا تزال مبرمجة ، ذلك بأنها غـير معـدة أصـلا لتقـديمها للتعامل .

وعلى أية حال فإن الأطراف قد يتفقوا على أن تكون للبيانات المدونة في الكمبيوتر حجة فيمـا بيـنهم في الإثبـات. ونـرى رغـم ذلـك أن الحمايـة الجنائية تختلف عن الحماية المدنية. هذا النوع الأخير من الحماية يتوقف على إرادة الأطراف ، أما الحماية الجنائية فإنها مقررة للمصلحة العامة التي ترتبط بالثقة في المحررات[1].

٥١- إدخال بيانات الكمبيوتر ضمن المحررات بنص خاص:

حرصت بعض التشريعات على إدخال بيانات الكمبيـوتر ضـمن طائفـة المحررات في مفهوم جريمة التزوير، بغض النظر عن المادة التي سجلت عليهـا تلك البيانات. فسواء سُجلت تلك البيانات على اسطوانة أو ديسك أو على أوراق أو كانت مدونة في الجهاز نفسه ، فإن وصف المحرر يسري عليها. مـن هذه التشريعات قانون العقوبات الكندي الذي ينص الفصل ٣٢١ منه على أن "المحرر يعني أوراق أو أي مادة أخرى مسجل أو مدون عليهـا مـا يمكـن قراءته أو فهمه من جانب الأشخاص أو أجهزة الكمبيوتر أو أي جهاز آخر. ويشمل ذلك كارت السحب الآلي . ولكنه لا يشمل العلامات التجارية التي يتم وضعها على السلع التجارية ، كما لا يشمل ما يُسجل على الحجارة أو المعادن أو غيرها من المواد المماثلة "[2].

---

(١) د. احمد حسام طه تمام ، المرجع السابق ، ص ٤٢٩ .

(2) The definition of " document " in section 321 states :
"Document means any paper, parchment or other material on which is recorded or marked anything that is capable of being read or understood by a person, computer system or other device, and includes a credit card, but does not include trade marks on articles of commerce or inscriptions on stone or metal or other like material " .

٥٢- الشروع في التزوير بالكذب في البيانات المبرمجة :

لا يحول القول بعدم وقوع جريمة التزوير في البيانات المبرمجة ، إذا قلنا بعدم اكتساب هذه البيانات لصفة المحرر، دون العقاب على كتابة بيانات كاذبة في نظام الكمبيوتر بوصفها شروعا في تزوير. ويلزم لذلك أن تكون هذه البيانات معدة لإخراج محررات بالمعني المعرّف به في جريمة التزوير.

ويعيب هذا الحل أنه لا يحمي نظام الكمبيوتر في حد ذاته أي البيانات المبرمجة في الكمبيوتر أو على أشرطة أو اسطوانات. هذا النظام يستحق الحماية الجنائية من العبث به ، حتى ولو لم تكون البيانات المدوّنة به معدة لإخراج مستندات.

٥٣- الحاجة إلى نصوص خاصة لحماية المعلومات المبرمجة من العبث بها :

أدرك المشرع الفرنسي أن ثمة صعوبة قانونية تُثار بسبب ظهور المعلومات المبرمجة من حيث اعتبارها محررا في مفهوم جريمة التزوير. لذا فقد أورد نصا خاصا للعقاب على تغيير الحقيقة في هذه المعلومات بمقتضى القانون رقم ٨٨ – ١٩ الصادر في ٥ يناير سنة ١٩٨٨ . وقد نص هذا القانون في المادة ٤٦٢/ ٥ على أن " كل من قام بتزوير وثائق المعلومات المبرمجة ، أيا كان شكلها ، إضرارا بالغير يعاقب بالحبس مدة لا تزيد على ٥ سنوات ولا تقل عن سنة واحدة وبالغرامة من ٢٠ ألف فرنك إلى ٢ مليون فرنك أو بإحدى هاتين العقوبتين "[1].

ويلاحظ أن قانون العقوبات الفرنسي قد أعاد تنظيم النصوص الخاصة

---

(1) quiconque aura procédé à la falsification de documents informatisés , quelle que soit leur forme , de nature à causer un préjudice à autrui , sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20 000 F à 2 000 000 F .

بالمعلومات المعالجة وفقا للقانون رقم ٨٨ / ١٩ الصادر في ٥ يناير سنة ١٩٨٨ والتي كانت واردة في الفصل الثالث بعنوان " في شأن بعض الجرائم في مواد الكمبيوتر " " De certaines infractions en matière informatique " . بدلا من ذلك أصبح قانون العقوبات الفرنسي يعالج هذه النصوص في هذا الباب الثالث بعنوان " الإخلال بنظم المعلومات المبرمجة "" Des atteintes aux systèmes de traitement automatisé des données " . وقد عمد المشرع الفرنسي عند إعادة هذه الصياغة إلى عدم ذكر المادة ٤٥٢ / ٥ والتي كانت تعاقب على تزوير المستندات المبرمجة وإلى عدم ذكر المادة ٤٦٢/ ٦ والتي تعاقب على استعمال المستندات المبرمجة التي تمّ تزويرها طبقا للمادة السابقة.

بيد أن ذلك لا يعني عدولا من المشرع الفرنسي عن اعتبار المعلومات المبرمجة بمثابة محررات في مفهوم جريمة التزوير. ولكنه أعاد تنظيم مواد التجريم في قانون العقوبات الجديد، بحيث عدّل النص الأصلي في التزوير لكي يشمل المعلومات المبرمجة. فتعرّف المادة ٤٤١ – ١ من قانون العقوبات الجديد التزوير بأنه كل تغيير للحقيقة ، بسوء نية ، من شأنه الإضرار بالغير ، أيا كانت الوسيلة المتبعة ، في مستند مكتوب أو في أي دعامة من دعائم التعبير عن الفكر التي لها شأن في إثبات حق أو واقعة لها نتائج قانونية [(١)] .

ويسمح هذا النص الجديد بسريان أحكام جريمة التزوير على تغيير الحقيقة في المعلومات المبرمجة ، حاسما أمر اعتبار هذه المعلومات من المحررات

---

(1) " constitue un faux toute altération frauduleuse de la vérité de nature à causer un préjudice et accomplie par quelconque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour objet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques " .

. فلا شيء يحول إذن دون القول بوقوع جريمة التزوير في محررات رسمية بتغيير الحقيقة في المعلومات المبرمجة في مصلحة حكومية، مثال ذلك درجات الطلاب المسجلة في كمبيوتر الجامعة. وذلك حتى ولو لم يتم إخراجها في شكل أوراق ، أي منذ حدوث هذا التغيير للحقيقة في المعلومات الخاصة بهذه الدرجات في الجهاز نفسه أو في الأشرطة أو الاسطوانات الخاصة بها.

وقد عنيت تشريعات أخرى باعتبار المعلومات المبرمجة من قبيل المحررات في مفهوم جريمة التزوير. من تلك التشريعات القانون الكندي(١) وفقا لتعديل قانون العقوبات الكندي في سنة ١٩٨٥ (٢) . فقد نص هذا التعديل على اعتبار من قبيل المحررات في جريمة التزوير " كل مادة يُسجل عليها ما يمكن قراءته أو فهمه من قبيل إنسان أو جهاز كمبيوتر أو أي جهاز آخر "(٣). وكان قانون العقوبات الأسترالي قد تم تعديله في سنة ١٩٨٣ (٤) لكي يعاقب في الفصل ٢٧٦ منه بالحبس مدة لا تزيد على ثلاث سنوات " كل شخص يقوم بتغيير أو تزوير أو مسح أو إتلاف أية بيانات مبرمجة بسوء نية " (٥) . كما تضمن القانون الإسرائيلي نصا على اعتبار المعلومات المبرمجة من قبيل المحررات في مفهوم جريمة تزوير المحررات(٦).

---

(١) انظر

Ultrich Sieber, id , at 47 .

(2) The Canadian Criminal Law Amendment Act of 1985 .

(3) " material , on which is recorded or marked anything that is capable of being read or understood by a person, computer system or other device " .

(٤) انظر

Ultrich Sieber, id , at 46.

(5) " any person who unlawfully alters , falsifies , erases or destroys any data processing material with any fraudulent intention " .

(٦) انظر :

Cole Durham , The emerging Structures of Criminal Information Law , General Report , in " Délits informatiques et autres infractions à la technologie de l'information", Colloque préparatoire, Wurzbourg (Allemagne) , Rev. int. dr. pén. 1993, p. 107.

ومع وجود هذا النوع من النصوص الذي حسم الجدل حول انطباق جريمة التزوير على المعلومات المبرمجة ، فإن ذلك لا يعني أن كل تغيير في هذه المعلومات يسري عليه جريمة التزوير. ذلك أن انطباق وصف التزوير منوط بتحقق شروطه ومن أهم تلك الشروط أن يكون لهذه البيانات شأن في الإثبات . وهذا لا يتوافر في كثير من البيانات التي تقدمها جهات عديدة بغرض استغلالها تجاريا وعلميا . فقد شهدت الآونة الأخيرة ظهور برامج تعدها كثير من الجهات أو الشركات للاستعمال الداخلي في تلك الجهة أو الشركة . عندئذ لا تمتد إليها الحماية بوصف التزوير . كما أن كثيرا من الأفراد أو الشركات تستعين بالبرامج التي أعدها مقدمو تلك البرامج والتي يضعونها تحت تصرف الغير في نظير اشتراكات معينة . هذه البرامج ليست معدة لإخراج مستندات تصلح للاحتجاج بها. وبالتالي فإن تجريم التزوير ينحسر عنها في هذه الحالة . من هذه البرامج أيضا ما يُقدم عبر شبكة الإنترنت.

الفصل الثاني

ضرورة استحداث نصوص خاصة بالتجريم

لمكافحة جرائم الكمبيوتر والإنترنت

٥٤ – برهن العرض السابق على الحاجة إلى استحداث نصوص خاصة لمكافحة جرائم الكمبيوتر ، وأن مرد ذلك كان إلى سببين:

السبب الأول : وجود صعوبات قانونية تتعلق بتطبيق الأحكام العامة المتعلقة بالجرائم التقليدية (كجرائم الأموال وتزوير المحررات) في مجال جرائم الكمبيوتر.

السبب الثاني : ظهور صور جديدة من الأنشطة الإجرامية التي اقترنت بصفة خاصة بالانتشار الواسع في استعمال الكمبيوتر والتي جعلت تدخل المشرع بنصوص خاصة أمرا حتميا.

فقد اقترن ظهور وانتشار أجهزة الكمبيوتر إلى ازدياد المخاطر التي يتسبب فيها للحياة الخاصة بالأفراد . وقد استلزم ذلك سن تشريعات تنظم استعمال هذه الأجهزة حتى لا تصبح مصدرا للاعتداء على الحياة الخاصة .

يضاف إلى ذلك استشعار الحاجة إلى حماية نظام الكمبيوتر من التداخل فيه والاطلاع علي ما به من معلومات يحرص صاحبها على الاستئثار بها . كما أنه كان من الواجب حماية المعلومات المبرمجة بهذا النظام من التغيير أو الإتلاف ، الأمر الذي لا تفي القواعد العامة دائما به .

وأخيرا ظهرت خدمات هامة تقدمها شركات خاصة في شكل برامج ترسلها عبر شبكة الإنترنت الدولية أو الدوائر الداخلية وتتقاضى اشتراكات

مقابـل هـذه الخـدمات. وقـد أدرك المـشرع في دول كـثيرة أن الأمـر يتعلـق بمصلحة اجتماعية ينبغي التدخل بنصوص خاصة لحمايتها .

وسوف نعالج في المباحث التالية الجوانب الثلاثة التي تدخل المشرع في بلدان عديدة بنصوص جنائية في صددها ، وهي : حمايـة الحريـة الشخـصية للأفراد (في المبحث الأول) ، وحماية نظام الكمبيوتر (المبحث الثاني)، وضرورة الأخذ في الاعتبار الوضع الخاص لاستعمال الإنترنت في ارتكاب الجرائم .

المبحث الأول
ضرورة حماية الأفراد من تجميع بيانات شخصية عنهم بطريق الكمبيوتر

٥٥ - المقصود بالبيانات الشخصية:

يقصد بالبيانات الشخصية أو الاسمية informations nominatives تلك البيانات التي تتعلق بشخص معين [(١)]. ولا يشترط في هذه البيانات أن تكون متعلقة بالحياة الخاصة للأفراد. بل إنه يكفي أن تتعلق بالحياة المهنية للفرد أو حتى بحياته العامة أو انتماءاته السياسية أو النقابية المعروفة [(٢)(٣)] . وإذا تعلقت المعلومات بالحياة الخاصة للأفراد كأصوله العنصرية وحالته الطبية وسوابقه القضائية ، فإن هناك حظرا يفرضه القانون وليس مجرد تنظيم لعملية جمع تلك المعلومات.

وبناء عليه فإن القوانين التي تنظم جمع معلومات عن الأشخاص وبرمجتها بواسطة الكمبيوتر لا ترمي فقط إلى حماية الجانب الداخلي من حياته الخاصة فقط، بل إلى احترام كل ما يتعلق به ، احتراما لحريته الشخصية وليس اقتصارا على حياته الخاصة(٤).

---

(١) د. حسام الدين كامل الأهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي، مؤتمر جامعة الكويت حول " القانون والحاسب الآلي " ، مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي ١٩٩٤ ص ١١٣ .

(2) Raymond GASSIN, " La protection pénale des informations sur la personne en droit français contemporain" in " Droit pénal contemportain " Mélanges en l'honneur d'André Vitu , éd. Cujas 1989 , p. 237 .

(٣) د. محمد عبد المحسن المقاطع ، نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر ، مؤتمر جامعة الكويت حول " القانون والحاسب الآلي " مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي ، ١٩٩٤ ص ١٨٨ .

(٤) د. محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد و ضماناتها في مواجهة الحاسوب الآلي ، مطبوعات جامعة الكويت ، مجلس النشر العلمي ، ١٩٩٢ .

٥٦- الفرد محل الحماية وليس الشخص المعنوي:

يحمي قانون الكمبيوتر والحريات في فرنسا الشخص الطبيعي وليس الشخص المعنوي ، باعتبار أن المقصود هو حماية الحريات الشخصية ، الأمر الذي لا يتوافر فيما يتعلق بالأشخاص المعنوية مثل الشركات والجمعيات وغيرها من التجمعات [١]. وقد أفصح المشرع الفرنسي عن ذلك صراحة عندما تعرض لتعريف المعلومات الشخصية (الاسمية) nominatives في المادة الرابعة من القانون رقم ٧٨ - ١٧ الصادر في ٦ يناير سنة ١٩٧٨ في خصوص الكمبيوتر والحريات بقوله " تعتبر اسميه في مفهوم هذا القانون المعلومات التي تسمح بطريقة أو بأخرى ، وسواء كان ذلك بشكل مباشر أو غير مباشر ، بتحديد الشخص الطبيعي الذي تتعلق به ، يستوي في ذلك أن يكون القائم بتجميع تلك المعلومات شخص طبيعي أو شخص معنوي " [٢].

ويلاحظ أن موقف القانون الفرنسي في اقتصاره على حماية الشخص الطبيعي دون الشخص المعنوي من جمع المعلومات الخاصة به لا يشاطره تشريعات أوربية أخرى مثل النرويج والنمسا وإيرلندا ولكسمبورج والدنمارك [٣].

---

(1) Jacques FRANCILLON ," L'adaptation du droit pénal à certaines fromes de délinquance informatiques et audio-visuelles " in " La protection pénale des infromations sur la personne en droit français contemporain , in " Droit pénal contemporain " Mélanges en l'honneur d'André Vitu , éd. Cujas 1989.

(2) " sont réputées nominatives au sens de la présente loi les informations qui permettent , sous quelque forme que ce soit, directement ou non, l'identification des personnes pysiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne pysique ou par une personne morale ".

(٣) مشار إليه في : د. محمد عبد المحسن المقاطع ، نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر ، أعمال مؤتمر الكويت ، المرجع السابق ، ص ١٨٦ .

٥٧ - خطورة جمع المعلومات الشخصية بالنسبة للحريات الأفراد:

أراد المشرع بهذا التنظيم احترام رغبة الأفراد في عدم اطلاع الغير على بيانات خاصة بهم أو عدم تعميم تلك المعلومات التي تمسهم . فمكان إقامة الشخص وعنوانه وطبيعة عمله ومستوى تعليمه وديانته ومقدار دخله ورقم تليفونه وحالته الاجتماعية من حيث كونه متزوجا أو غير ذلك، ومن حيث وجود أو عدم وجود أبناء له و حالة صحيفته الجنائية (صحيفة السوابق) وغيرها من المعلومات الخاصة لها طابع شخصي مادام صاحبها لا يرغب في اطلاع الغير عليها .

٥٨- اختلاف المعلومات الشخصية عن المعلومات السرية:

تختلف المعلومات الشخصية عن المعلومات السرية . فما يتعلق بصحيفة الحالة الجنائية يُعد من الأسرار لدى المصلحة المختصة بها بوزارة الداخلية . وكذلك الأمر بالنسبة لدخل الفرد . هذا الدخل يعتبر من الأسرار لدى مأموري الضرائب. هؤلاء يلتزمون بسرية مهنتهم بخصوص دخول الأفراد ويسألون وفقا للمادة ٣١٠ من قانون العقوبات. هذه المادة تنص على أن " كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم مودعا إليه بمقتضى صناعته أو وظيفته سر خصوصي ائتمن عليه فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك يعاقب بالحبس مدة لا تزيد على ستة شهور أو بغرامة لا تتجاوز خمسمائة جنيه مصري ....." [(١)].

هذه المعلومات الشخصية تستحق الحماية التي يقررها القانون لكفالة

---

(١) د. غنام محمد غنام ، الحماية الجنائية للأسرار الأفراد لدى الموظف العام ، دار النهضة العربية ، ١٩٨٨ ، ص ٤٢.

حرمة الحياة الخاصة . مع ذلك فإن هذه الفكرة تعتبر من الأفكار الجديدة بالنسبة للقواعد التقليدية في قانون العقوبات . هذا القانون لا يمد حمايته للحياة الخاصة إلاّ بالنظر إلى المكان الخاص الذي يرتبط بالحياة الخاصة للشخص (¹). لذا تنص المادة ٣٠٩ مكررا عقوبات في مصر على عقاب من استرق السمع أو سجّل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون . وكذلك يعاقب بنفس العقوبة كل من التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص . فحرمة الحياة الخاصة مرتبطة وفقا للمفهوم التقليدي بحرمة المكان الخاص. وهنا يأتي التجديد الذي ساهم في ظهوره نظام المعلومات المبرمجة (الكمبيوتر).

٥٩ - اختلاف المعلومات الشخصية عن المعلومات المتعلقة بسمعة الأفراد وشرفهم :

تختلف المعلومات الشخصية عن المعلومات التي تتعلق بسمعة الأشخاص واعتبارهم . فالمعلومات الشخصية قد تتعلق بسمعة الأفراد واعتبارهم وقد لا تتعلق. فرقم تليفون منزل أحد الشخص لا يتعلق بسمعته واعتباره ، أما سبق صدور حكم جنائي ضده فإنه أمر يتعلق بسمعته واعتباره . وقد أورد قانون العقوبات التقليدي من الأحكام ما يحمي سمعة الأفراد واعتبارهم ضد من يُسند إليهم – وخاصة بشكل علني – أمور لو صحت لاستوجبت احتقارهم لدى بني وطنهم . أما المعلومات الشخصية ،فإنها تحتاج إلى تلك الحماية الجنائية التي لا تكفلها القواعد التقليدية في قانون العقوبات لأنها لا تمس الشرف والاعتبار ، ولأنه لم يتم نشرها بطريق من طرق العلانية، ولأنها

---

(١) د. عمر الفاروق الحسيني ، المرجع السابق ص ٦٠ .

ليست معلومات ذات طابع سري. لذا لا يبقى سوى إدخال نصوص خاصة لتحقيق تلك الغاية.

وقد ظهرت مخاطر لحريات الأفراد بسبب جمع معلومات شخصية عن الأفراد قبل ظهور وانتشار أجهزة الكمبيوتر والاستعانة بها في تخزين هذه المعلومات . وازدادت هذه المخاطر مع انتشار استعمال الكمبيوتر . لذا فقد أدخل المشرع الفرنسي القانون رقم ٦ يناير لسنة ١٩٧٨ في شأن " الكمبيوتر والفيش والحريات " relative à l'informatique , aux fichiers et aux libertés.

وتزداد خطورة جمع هذه المعلومات الشخصية من ظهور شركات خاصة تعمل في مجال الأمن وتقوم بتجميع بيانات عن الأفراد لوضعها تحت تصرف من يريد أن يعرفها نظير دفع مقابل مالي . فقد أصبح وجود هذه المعلومات الشخصية مهددا للحياة الخاصة بالنسبة للفرد العادي وكذلك بالنسبة للشخصيات العامة . هذا التهديد للحياة الخاصة يتحقق سواء كانت هذه المعلومات كاذبة أو كانت صحيحة ، مادام صاحب الشأن يعترض على من يقوم بجمعها وتخزينها أو يقوم بتزويد الآخرين بها بدون مبرر قانوني مقبول.

٦٠- اهتمام التشريعات المختلفة بحماية الحرية الشخصية للأفراد:

تهتم التشريعات المختلفة في الوضع الراهن بحماية الحرية الشخصية من إساءة استعمال الكمبيوتر عند جمع المعلومات الشخصية عن الأفراد . لذلك فإنها تقوم بتنظيم مثل ذلك النشاط . من ذلك التشريع الفرنسي الصادر في ٦ يناير سنة ١٩٧٨ . كما أن دول المجلس الأوربي قد انضمت إلى الاتفاقية

الأوربية لحماية الأفراد من المعلومات المبرمجة ذات الطابع الشخصي . تلك هي اتفاقية ٢٨ من يناير سنة ١٩٨١ [1].

٦١- المقصود بالمعلومات المبرمجة والمعلومات المعالجة يدويا :

تتعلق بعض نصوص التجريم المعلومات المبرمجة بصفة خاصة، بينما تسري نصوص أخرى للتجريم على المعلومات سواء منها ما تمت برمجته في الحاسب الآلي أو ما يتم معالجته يدويا " نظام الفيش ".

ويقصد بالمعلومات المبرمجة تلك التي تم إدخالها إلى نظام الكمبيوتر وتسجيلها على دعامة مادية مثل الشريط الممغنط أو في داخل الجهاز نفسه. كما تشمل عملية البرمجة للمعلومات كل ما يتعلق بحفظ تلك المعلومات في الذاكرة و إعدادها وتنسيقها وتوصيلها إلى علم الغير communication [2]. تطبيقا لذلك قُضي في فرنسا بأن مجرد إدخال البيانات في الكمبيوتر لا يحقق لها وصف البيانات المبرمجة ، إذا كان ذلك لا يعدو أن يكون كتابة لتلك البيانات وكان الغرض منها طبعها على ورق ليس الاحتفاظ بها في الجهاز[3]. وقد تعلق الأمر في هذه القضية ببيانات نُقلت من بعض ملفات المرضى وأراد الطبيب طباعتها على ورق لتسهيل تجميعها.

٦٢- وسائل حماية الإفراد من إساءة استعمال الكمبيوتر :

تصورت التشريعات المقارنة وسيلتين لحماية الأفراد من إساءة استعمال أنظمة الكمبيوتر. إحدى هاتين الوسيلتين وقائية والوسيلة الأخرى جزائية ، وسوف نبين ذلك على ما سيلي.

(1) Jérôme Huet , Herbert Maisl, Droit de l'informatique et de télécommunications, Litec,1989, p. 147.
(2)Gassin Raymond , " La protection pénale des informations sur la personne en droit français contemportain " , in " Droit pénal contemporain " , Mélanges en l'honneur d'André Vitu , éd. Cujas , 1989, p. 237 .
(3)Crim. 6 juill. 1994,cite par Jacques FRANCILLON, " Infractions relevant du droit de l'information et de la communication "Rev.sc.crim.1996, chronique de jurisprudence, p. 676.

المطلب الأول

الحماية الوقائية عن طريق التدابير الإدارية

٦٣ - أوردت كثير من التشريعات تدابير إدارية ترمي إلى حماية الحريات الشخصية للأفراد من التعسف في جمع وبرمجة المعلومات الشخصية . تتمثل هذه التدابير في تنظيمات إدارية تشكل ضمانة من الضمانات التي تكفل الحرية الشخصية للأفراد [1] .

من هذه التنظيمات ما يلي:

أولا – حظر جمع بعض المعلومات:

٦٤ – تكتسب بعض المعلومات أهمية خاصة دعت المشرع إلى حظر جمعها في نظام للمعلومات المبرمجة في الكمبيوتر أو حتى وفقا لنظام الفيش اليدوي.

من هذه المعلومات ما هو ذات طابع شخصي بحت . ومنها ما يتعلق بالسوابق الجنائية .

ولا يقف المشرع الفرنسي وحيدا في حظره لبرمجة مثل هذه البيانات ذات الطابع الشخصي البحت . بل إن تشريعات أخرى كالقانون الدنمركي يورد قاعدة الحظر بخصوص تلك الطائفة من البيانات[2].

---

(١) د. إبراهيم الدسوقي أبو الليل ، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة ، مؤتمر جامعة الإمارات ، كلية الشريعة والقانون حول " القانون والكمبيوتر والإنترنت " في الفترة ١ – ٣ مايو سنة ٢٠٠٠ ص ٣٤ .

(٢) انظر section(٣) ٢ , (١٧)٤ من قانون Private Registers Act في الدانمرك .

١ – المعلومات ذات الطابع الشخصي البحت :

تلك هي المعلومات المتعلقة بالأصول العنصرية للشخص وبآرائه أو انتماءاته السياسية أو الدينية أو النقابية وتلك المعلومات المعلقة بأخلاقيات الشخص ذاته . وقد عبر عن ذلك الحظر القانون الفرنسي رقم ٧٨ – ١٧ الصادر في ٦ يناير سنة ١٩٧٨ الخاص بالكمبيوتر والفيش والحريات (مادة ٣١).

وعلى الرغم من وجود هذا الحظر فإن المشرع الفرنسي ارتأى أن يورد بعض الاستثناءات على هذا الحظر ، هذه الاستثناءات هي:

(أ) حق الجهات القضائية وكذلك الإدارية ذات الاختصاص القضائي في الاحتفاظ بمعلومات مبرمجة تحتوي على عناصر من المعلومات المحظورة المشار إليها آنفا ، مادام ذلك لازما للفصل فيما تختص به هذه الجهات من نزاع.

(ب) حق الكنائس والجهات ذات الطابع الديني أو السياسي أو الفلسفي أو النقابي في الاحتفاظ بمعلومات مبرمجة من النوع السابق.

٢ – المعلومات المتعلقة بالسوابق القضائية :

من الطبيعي أن يحرص المشرع على المعلومات المتعلقة بالأحكام الجنائية الصادرة على الأفراد ، سواء تضمنت عقوبات أو تدابير ، وذلك على الرغم من أن هذه الأحكام تصدر في علانية.

وحرص المشرع على هذا النوع من الأحكام يتجلى في مظهرين:

المظهر الأول – الحماية وفقا لسرية المهنة :

يعتبر الموظفون القائمون على المعلومات الخاصة بالسوابق القضائية من

الأمناء على الأسرار الذين يلتزمون بالمحافظة على سرية هذه المعلومات[1] . وبالتالي فإنهم يُسألون وفقا للمادة ٣١٠ من قانون العقوبات في حالة إفشائهم لسرية هذه المعلومات.

المظهر الثاني – الحماية وفقا لقانون الكمبيوتر والحريات:

أورد قانون الكمبيوتر والحريات في فرنسا نصا خاصا بالمعلومات المتعلقة بالسوابق القضائية سواء منها الأحكام الجنائية أو التدابير. هذا النص يحظر جمع هذا النوع من المعلومات ، ويحظر الاحتفاظ بها ، كما يحظر اطلاع الغير عليها.

ومع ذلك فقد صرح القانون لنوعين من الجهات بجمع والاحتفاظ بهذا النوع من المعلومات، هما :

١ – الجهات القضائية والجهات العامة الأخرى التي يصرح لها القانون بالاحتفاظ بهذا النوع من المعلومات.

٢ – شركات التأمين . والمعروف أن هذه الشركات تحرص على معرفة معلومات شخصية عن راغبي التأمين على حياتهم أو على سياراتهم وعلى أموالهم بوجه عام.

ثانيا – النص على وضع خاص بالمعلومات الطبية:

٦٥ – من الواضح أن المعلومات الطبية تتميز بوضع خاص بين المعلومات الشخصية نظرا لتعلقها بما يصاب الفرد من أمراض. ومن المعروف أن هذه المعلومات تحميها المادة ٣١٠ عقوبات الخاصة بإفشاء أسرار

---

(١) د. غنام محمد غنام ، الحماية الجنائية لأسرار الأفراد لدى الموظف العام ، المرجع السابق ، ص ٥٢ .

المهنة، وذلك إذا قام أحد أفراد المهنة الطبية (طبيب، ممرض، قابلة) بإفشاء شيء من هذه المعلومات إلى شخص الغير في غير الحالات التي يلزمه القانون بذلك.

لكن الجديد الذي أتى به قانون الكمبيوتر والحريات في فرنسا هو تنظيم جمع هذه المعلومات الطبية سواء في نظام للكمبيوتر أو نظام يدوي لجمع المعلومات.

وتقضي القاعدة العامة التي وضعها قانون الكمبيوتر والحريات - بعد تعديله بمقتضى القانون الصادر في أول يوليو سنة ١٩٩٤ - في خصوص هذه الطائفة من المعلومات أن جمع والاحتفاظ بهذه المعلومات مقصور على حالتين:

الحالة الأولى : حالة متابعة المرضى طبيا . تلك هي الحالة التي فيها يقوم الأطباء بتدوين بيانات عن مرضاهم ، سواء كان هذا التجميع يدويا أو في نظام الكمبيوتر .

الحالة الثانية : حالة البحث العلمي . أقر قانون الكمبيوتر والحريات بمقتضى التعديل الصادر في أول يوليو سنة ١٩٩٤ الضرورة العلمية التي تقتضي أن تقوم مراكز البحث العلمي بتجمع والاحتفاظ ببيانات تتعلق بصحة الأفراد .

ثالثا – تنظيم جمع المعلومات والاحتفاظ بها :

٦٦- فيما عدا الأنواع السابقة من المعلومات التي أفرد لها القانون الفرنسي وضعا خاصا، تكفّل قانون الكمبيوتر والحريات بوضع تنظيمات عامة لجمع المعلومات الشخصية والاحتفاظ سواء تم ذلك بطريقة يدوية في

أوراق أو كان ذلك بتسجيل هذه المعلومات في نظام الكمبيوتر.

من أهم التنظيمات التي وضعها القانون الفرنسي المشار إليه ما يلي :

١-واجب الإخطار:

٦٧ -تفرض المادة ١٦ من قانون الكمبيوتر والحريات التزاماً على كل شخص يقوم بتسجيل معلومات شخصية عن الأفراد أن يخطر لجنة إدارية خاصة أنشأها القانون لمراقبة مدى احترام الحياة الخاصة للأفراد ، تلك هي " اللجنة الوطنية للكمبيوتر والحريات " (مادة ١٦) . ويلاحظ أن القانون يفرض واجب الإخطار قبل القيام بإدخال المعلومات في الكمبيوتر وليس قبل جمع هذه المعلومات. كما يلاحظ أن القانون لا يستلزم موافقة اللجنة قبل القيام بعملية التسجيل المشار إليها ، وإنما مجرد إخطارها. وعند إخطار اللجنة على هذا النحو تقوم بمتابعة مهمتها في التحقق من مدى احترام الأحكام المقررة في هذا القانون.

ومن الجدير بالذكر أن واجب الإخطار المشار إليه في الفقرة السابقة لا يقع على الجهات العامة. هذه الجهات ينظم عملها في جمع المعلومات الشخصية ومعالجتها في أجهزة الكمبيوتر لوائح خاصة (مادة ١٥ ومادة٢٠).

ويشارك القانون الفرنسي تشريعات أوربية عديدة في اشتراطها أن يتم هذا النوع من الإخطار إلى جهة تتولى مهمة المراقبة والمتابعة حماية للحياة الخاصة للأفراد(١). من ذلك القانون الدنمركي (٢) والقانون السويدي (٣) وقانون لكسمبورج (٤) والقانون الإيطالي(٥).

---

(١) انظر
Ulrich Sieber , id at 107.

(٢) انظر
section 8 , 20 (1) and (2), 21 (2) and 27 (2) n° 4 .

(٣) انظر
section 20 (1) and (2) , Swedish Data Act.

(٤) انظر
section 32 , Luxembourgian Act Regulating the Use of Nominal Data

(٥) انظر
section 23

٢ – تجميع المعلومات بأسلوب مشروع:

٦٨– يتعين أن يتم تجميع المعلومات بأسلوب لا يتسم بالغش أو بأي أسلوب آخر غير مشروع أو غير أمين . على ذلك نصت المادة ٢٥ من قانون الكمبيوتر والحريات في فرنسا.

٣ – حق صاحب الشأن في الاعتراض على تسجيل المعلومات الخاصة به:

٦٩– أقر قانون الكمبيوتر والحريات في فرنسا حق صاحب الشأن الذي تتعلق المعلومات به أن يعترض على تسجيل هذه البيانات والتعامل فيها بطريق الكمبيوتر، مادام لديه أسباب مقبولة لذلك. وقد أشار القانون السابق إلى أن حق الاعتراض لا يسري في مواجهة الجهات العامة . هذه الجهات تستمد حقها في تجميع المعلومات ومعالجتها من لائحة تقر لها بهذا الحق.

٤ – حق صاحب الشأن في الاطلاع:

٧٠ – إذا لم يعترض صاحب الشأن على تسجيل البيانات الخاصة به لعدم علمه بتجميعها عنه ، أو لعلمه وعدم اعتراضه ، فإن من حقه أن يطلب الاطلاع على ما يخصه من هذه المعلومات [1] ليعرف كنهها . كما أن من حقه أن يحصل على نسخة منها . وقد أقر قانون الكمبيوتر والحريات حق صاحب الشأن في تصحيح المعلومات الخاصة به ، بما يتضمنه ذلك من حذف ما هو غير صحيح أو ما هو غامض أو يبعث على اللبس منها (مادة ٣٤ وما يليها) .

---

(1) droit d'accès

المطلب الثاني

الحماية الجنائية عن طريق التجريم

٧١ - ضرورة التدخل العقابي بنصوص خاصة :

كان من الطبيعي أن يورد القانون الفرنسي جزاءات على مخالفة أحكامه . وقد أضافها المشرع الفرنسي بمقتضى القانون الصادر في ١٦ ديسمبر سنة ١٩٩٢ لتصير المواد ٢٢٦ - ١٦ وما يليها من قانون العقوبات الفرنسي[1].

٧٢ - التدخل العقابي يشمل البيانات الشخصية :

يحمي المشرع الفرنسي بالتجريم البيانات الشخصية المبرمجة أي تلك التي تتعلق به شخصيا . ولا يلزم أن تكون هذه البيانات سرية بطبيعتها . كما لا يلزم في القائم ببرمجة هذه البيانات أن ينتمي إلى طوائف الأمناء على الأسرار التي ورد ذكرها في المادة ٢٢٦- ١٣ من قانون العقوبات.

ولم يحدد القانون المقصود بالبيانات الشخصية التي يشملها التجريم . والأمر متروك للقاضي أن يقوم باستخلاص مفهوم تلك البيانات من خلال ما يتمتع به من سلطة في تفسير النصوص في ضوء معطيات الواقع. فالمسألة هي من مسائل القانون المختلطة بالواقع ، أي أنها من المسائل الموضوعية بتعبير آخر، يترك أمر تقديرها لقاضي الموضوع دون معقب عليه في ذلك من محكمة النقض ، إلاّ فيما يتعلق برقابة هذه المحكمة على تسبيب الأحكام.

تطبيقا لذلك قُضي بأن رقم تليفون منزل الشخص من البيانات

---

(١) رقم ٩٢ - ١٣٣٦ .

الشخصية التي تقع جريمة إفشاء البيانات المبرمجة بإفشائه إلى الغير[1].

فيكفي في البيان حتى يُعد شخصيا أن يسمح بتحديد الشخص المقصود به سواء كان ذلك بشكل مباشر أو بشكل غير مباشر . بهذا قضت محكمة النقض الفرنسية ، غير مشترطة أن يتعلق البيان بالحياة الخاصة للفرد أو بجوانب معينة من شخصيته[2]. إعمالا لهذا المبدأ قضت المحكمة بتوافر صفة البيانات الشخصية لما قام به صاحب شركة تحصيل ديون من تجميع بيانات عن الأشخاص المدينين وتسجيلها في الكمبيوتر الخاص بشركته ، متضمنا ذلك اسم المدين ومحل إقامته ومبلغ دينه . كما قام المتهم بتجميع بيانات عن مدى يسار كل دائن من الناحية المالية [3] .

٧٣- التدخل العقابي يشمل المعلومات غير الآلية أيضا :

يُلاحظ أن أحكام الحماية الجنائية المقررة في قانون الكمبيوتر والفيش والحريات لا تنحصر في المعالجة الآلية للمعلومات عن طريق الكمبيوتر، وإنما تمتد في مجال تطبيقها إلى البيانات التي تسجل على فيش (أوراق) وذلك بالنسبة لبعض الجرائم التي حددتها المادة ٢٢٦ – ٢٣ من قانون العقوبات الفرنسي وهي الجرائم الواردة في المواد ٢٢٦ – ١٧ ، و٢٢٦- ١٨ و٢٢٦- ١٩ عقوبات . ولكنه ليس من بين هذه الجرائم جريمة مخالفة القواعد السابقة على برمجة البيانات (أي عدم إخطار لجنة الحريات والكمبيوتر).

(1) Trib. Corr. Briey , 15 sept. 1992; D. 1994 . Somm. 289.obs. Maisl; Gaz. Pal . 1993 . I. 201 et la note , et 1994. I. Somm. 107 .

(2) Cass. crim. 3 nov. 1987, D. j. 17, note Herbert Maisl.

(3) Crim 3 nov. 1987, op.cit.

٧٤- جرائم حماية الحياة الخاصة من إساءة استعمال الكمبيوتر من جرائم الأشخاص:

أورد قانون العقوبات الفرنسي هذا النوع من الجرائم تحت عنوان "المساس بحقوق الأشخاص الناتج عن استعمال الفيش ومعالجة المعلومات" . ومؤدى ذلك أن هذه الطائفة من الجرائم هي من جرائم الأشخاص . يترتب على ذلك أن المجني عليه في هذه الجرائم هو الشخص المقصود بالمعلومات، وذلك بالإضافة إلى المصلحة العامة والمتمثلة في مخالفة الإجراءات واجبة الاتباع قبل معالجة المعلومات.

٧٥- جرائم إساءة استعمال الكمبيوتر:

مادامت المعالجة الآلية للبيانات تشكل الركن المادي في جرائم إساءة استعمال الكمبيوتر ، بالإضافة إلى عناصر أخرى مثل عدم رضاء صاحب الشأن، ومادامت المعالجة الآلية للبيانات تتحقق بتواجد المعلومات في النظام (الكمبيوتر)، فإن مؤدى ذلك أن هذه الجرائم من الجرائم المستمرة.

من أهم صور التجريم التي تحمي الحياة الخاصة من إساءة استعمال الكمبيوتر ما يلي:

أولا - مخالفة القواعد السابقة على برمجة المعلومات :

٧٦- من ذلك أن يقوم أحد الأشخاص ببرمجة المعلومات ، أي إدخالها إلى الكمبيوتر أو نقلها منه على شريط دون إخطار الجهة المشار إليها في القانون.

ويقصد بالجهة المشار إليها في القانون " لجنة الكمبيوتر والحريات ". كما لا يجوز تجميع ومعالجة البيانات الشخصية للأفراد لحساب إدارة من

الإدارات العامة إلا بمقتضى لائحة تسمح بذلك وفقا للإجراءات المنصوص عليها قانونا ، ومنها أخذ رأي لجنة الكمبيوتر والحريات (مادة ١٥ من قانون الكمبيوتر والفيش والحريات الصادر في ٦ يناير سنة ١٩٧٨) . وقد رتب القضاء الفرنسي على ذلك أنه إذا قامت إحدى الإدارات بتجميع صور شخصية وبصمات المتهمين بعد موافقة لجنة الكمبيوتر والحريات وذلك بشكل تجريبي ، أي لمدة مؤقتة ، فإن انقضاء المدة المحددة لموافقة اللجنة تعطي أصحاب هذه الصور والبصمات الحق في حذف بياناتهم من سجل الكمبيوتر بهذه الجهة(١).

ويلاحظ أن نص التجريم الخاص بمعالجة المعلومات قبل إخطار لجنة الكمبيوتر والحريات لا ينسحب على تجميع المعلومات اليدوية . ويرجع ذلك إلى نص المادة ٢٢٦ – ٢٣ عقوبات فرنسي التي أشارت إلى التسوية بين البيانات المبرمجة والبيانات المعالجة يدويا في خصوص بعض الجرائم التي ليس من بينها هذه الجريمة. وقد قُضي بالفعل في فرنسا بذلك نظرا لاقتصار النص على هذه الطائفة من المعلومات (٢) وقد أوردت المادة ٢٢٦- ١٦ من قانون العقوبات الفرنسي عقوبة الحبس ثلاث سنوات والغرامة التي لا تزيد على ٣٠٠ ألف فرنك.

ولا يقتصر الركن المادي في هذه الجريمة على إدخال المعلومات الشخصية في جهاز الكمبيوتر، بل يتوافر النشاط بكل معالجة لتلك المعلومات . ويقصد بتلك المعالجة كل نقل لهذه المعلومات من جهاز إلى جهاز ، ومن الجهاز إلى الشريط الممغنط . تطبيقا لذلك قُضي بوقوع الجريمة

(1) TGI. Marseille , 23 mars 1995, D. 1996 , 40 , note Frayssinet.

(2) Agen, 28 fév. 1994, J.C.P. 1994. IV. 2209.

ممن قام بنقل بيانات تخص أفراد ليسوا أعضاء في الجمعية التي يتبعها المتهم على شريط ممغنط من الكمبيوتر الذي كانت مدونة عليه [1].

وبالنسبة للركن المعنوي ، يُلاحظ أن المادة ٢٢٦ – ١٦ عقوبات فرنسي تعاقب كل من قام بمعالجة للمعلومات ، ولو بطريق الإهمال . وهنا يبين أن الجريمة تقع بالخطأ في بعض صورها بالإضافة إلى العمد . ومؤدى ذلك أن الجريمة تقع إذا قام المتهم بمعالجة هذه البيانات دون أن يتثبت ويتحرى عن الإجراءات واجبة الاتباع ، فالإهمال عندئذ متصور . أما إذا لم يُنسب إليه خطأ ، فإن الجريمة لا تقوم عندئذ وذلك لعدم توافر الركن المعنوي . ويخالف ذلك ما سبق أن قضت به محكمة النقض الفرنسية من وقوع الجريمة بناء على النشاط فقط، ودون ما تطلب للركن المعنوي . فقد اعتبرتها المحكمة من الجرائم المادية في ظل عقوبات الفرنسي قبل تعديله في سنة ١٩٩٢ [2] . فقد سبق أن قضت المحكمة بأنه لا يلزم توافر القصد الجنائي في هذه الجريمة وبأنه لا يجدي المتهم إلاّ التمسك بالقوة القاهرة لإعفائه من المسئولية الجنائية [3].

وقد تضمن القانون عقوبة أخرى لمن يقوم بالاحتفاظ بالمعلومات الشخصية في جهاز الكمبيوتر متجاوزا المدة المقررة في الإخطار المبين سابقا والذي يصدر عن القائم على تجميع البيانات وبرمجتها بغرض إحاطة لجنة الكمبيوتر والحريات علما بما يقوم به من تجميع للمعلومات الشخصية . في ذلك أوردت المادة ٢٢٦ – ٢٠ عقوبات فرنسي عقوبة الحبس مدة ثلاث سنوات والغرامة ٣٠٠ ألف فرنك.

---

(1) TGI , Lille , 18 déc. 1996; D. 1997, 373 .
(2) Crim. 3 nov. 1987, Bull. crim. n° 382; Rev. sc. crim. 1988. 295, obs. Delmas Saint- Hilaire ; J. C. P. 1988. 1. 3323 .
(3) Crim 3 nov. 1987 , D. 1988. J. 17, note Herbert Maisl.

وواضح من التنظيم القانوني لهذه الجريمة أنها تقع اعتداء على المصلحة العامة التي تقتضي ضرورة اتباع إجراءات معينة قبل معالجة المعلومات. ومع ذلك فإن المجني عليه في هذه الجريمة أيضا هو الأفراد المقصودين بالمعلومات الشخصية . ويتأكد هذا إذا علمنا أن النص على الجريمة قد ورد في الفصل الخامس تحت عنوان " المساس بحقوق الأفراد الناتج عن استعمال الفيش والكمبيوتر ". يترتب على ذلك أن للفرد المقصود بالبيانات الشخصية أن يدعي مدنيا أما القضاء الجنائي عن ضرر شخصي ومباشر. وقد انتهت إلى ذلك أحكام القضاء الفرنسي بالفعل [1] .

ثانيا – برمجة المعلومات الشخصية دون اتخاذ الاحتياطات اللازمة :

٧٧- تعاقب المادة ٢٢٦ – ١٧ عقوبات فرنسي على القيام ببرمجة المعلومات الشخصية دون اتخاذ ما يكفي من احتياطات للمحافظة على سلامة هذه المعلومات. فمن واجب القائم بتلك البرمجة أن يحول دون تشويه هذه المعلومات أو تحريفها أو اطلاع الغير عليها بدون وجه حق . والعقوبة المقررة لذلك الفعل هي الحبس خمس سنوات والغرامة التي لا تزيد على ٢ مليون فرنك.

ومن الجدير بالذكر أن هذا التجريم قد ورد في القانون الفرنسي مقتصرا على المعلومات المبرمجة . وبناء عليه لا تقع الجريمة إذا تعلق الأمر بالمعلومات التي يتم معالجتها بطريقة يدوية وذلك لأن النص لا ينسحب عليها [2].

وقد قُضي بأن المجني عليه في هذه الجريمة هو من يصاب بضرر مباشر منها بسبب عدم اتخاذ ما يلزم من إجراءات تكفل عدم مساسها بشخص

---

(1) Paris 13 sept. 1996. 677, obs. Francillon ; Dr. pénal 1996, 32, obs Véron
(2) Agen , 28 fév. 1994; J.C.P. 1994.IV.2209.

الغير[1]. لذا فإن الجريمة تقوم إذا قام مسئول بشركة ائتمان بتدوين بيانات عن شخص بوصفه من المدينين السيئين وترتب على عدم تدوين بيان محل الميلاد أن اختلط مع اسم شخص آخر يتشابه معه في الاسم ويختلف في بيان محل الميلاد. وقد انتهى القضاء الفرنسي في هذه القضية إلى أن هذا الشخص غير المقصود أصلا يعد مجنيا عليه ومضرورا أيضا من الجريمة[2].

ثالثا - برمجة معلومات شخصية رغم اعتراض صاحب الشأن:

٧٨ - لا يشترط عند تجميع معلومات شخصية عن الأفراد سبق الحصول على موافقة صريحة منهم على هذا التجميع وتلك البرمجة إلا بالنسبة للمعلومات المحظورة وهي المتعلقة بالأصل العنصري للشخص ومعتنقاته وآرائه الدينية والسياسية والفلسفية وانتماءاته النقابية. يكفي إذن إخطار لجنة الكمبيوتر والحريات. بيد أنه قد يخول القانون صاحب الشأن الحق في الاعتراض على برمجة هذه البيانات. عندئذ يتعرض للعقاب من يقوم بهذا التجميع أو تلك المعالجة رغم هذا الاعتراض. والعقوبة المقررة وفقا للمادة ٢٢٦ - ١٨ عقوبات فرنسي هي الحبس مدة لا تزيد على خمس سنوات والغرامة التي لا تزيد على ٢ مليون فرنك.

ولا يعني ما سبق أن القائم بتجميع البيانات وبرمجتها يقع عليه التزام بإخطار الشخص الذي تتعلق به البيانات الشخصية . بالتالي فإنه إذا قام بتجميع هذه البيانات وبرمجتها دون هذا القيام بهذا الإخطار فإنه لا يرتكب سلوكا مؤثما . لذا نقضت محكمة النقض حكم محكمة الاستئناف الذي

(1) Crim 19 déc. 1995; Bull. crim. n° 387; Rev. sc. crim.1996. 679, obs. Francillon ; Dr. pénal 1996. comm. 126, note Véron ; D. 1996. IR. 81.

(2) Crim. 19 déc. 1995, op.cit.

قضى بإدانة المتهم استنادا إلى هذا الأساس[1]. فالجريمة لا تقوم إلاّ عند اعتراض صاحب الشأن على المعلومات التي تخصه – مع وجود مبرر قانوني لذلك – وعدم حذف أو تعديل البيانات.

رابعا – إدخال معلومات شخصية محظورة دون موافقة صاحبها :

٧٩– تعاقب المادة ٢٢٦-١٩ من قانون العقوبات الفرنسي من يقوم ببرمجة (إدخال) معلومات تتعلق بالأصل العنصري للشخص أو بآرائه السياسية أو الدينية أو الفلسفية أو تتعلق بانتماءاته النقابية أو أخلاقياته العامة، وذلك إذا حدث ذلك بدون موافقة صريحة من صاحب الشأن . وقد قررت المادة السابقة عقوبة الحبس الذي لا يزيد على خمس سنوات والغرامة التي لا تزيد على ٢ مليون فرنك على مخالفة هذا الحظر.

ويسري نفس الحكم على المعلومات الشخصية المتعلقة بالعقوبات والتدابير الجنائية.

ومؤدى ذلك أن الجريمة تقوم من المتهم الذي يحرص على إخفاء ما يقوم به من أعمال تتمثل في تجميع البيانات الشخصية المحظورة أصلا ، دون إخطار لجنة الحريات ودون إعلام صاحب هذه البيانات حتى يحصل على موافقة منه[2].

ويستوي في وقوع الجريمة أن ترد هذه البيانات المحظورة في معلومات مبرمجة بطريق الكمبيوتر أو معالجة يدويا أي في شكل " فيش " . ويرجع ذلك إلى صريح نص المادة ٢٢٦ – ٢٣ من قانون العقوبات الفرنسي الذي

(1) Crim 25 oct. 1995, Bull.crim.n° 320 ; Rev. sc. crim. 1996, note Mole; Dr. pénal 1996. Comm. 86, note Véron .
(2) Crim. 4 mars 1997, Bull crim. n° 83; Rev. sc. crim. 1997, 669, obs. Dintilhac; J.C.P. 1997.IV.1612; Dr. pénal 1997. Comm. 75 , note Véron

أقام التسوية بين البيانات المبرمجة و" الفيش " أي البيانات المعالجة يدويا فيما يتعلق بهذه الجريمة .

وتحديد ما يعتبر من البيانات المبرمجة لا يثير صعوبة قانونية . والأمر على خلاف ذلك بالنسبة " للفيش " أي البيانات المعالجة يدويا . وتقدر محكمة الموضوع – وفقا لسلطتها التقديرية – ما إذا كانت الأوراق أو السجل الذي يمسكه المتهم له صفة " الفيش " المقصود بالتجريم . وتهتدي المحكمة في حكمها في هذا الخصوص بمدى حجم تلك الأوراق ومدى تنظيمها . كما لا تغفل المحكمة واقعة أن تلك الأوراق أو ذلك السجل يسمح بالرجوع إليها . وبناء عليه ، إذا تعلق الأمر بمجرد ملف أو عدد قليل من الملفات عن بعض الأشخاص ، فإن ذلك لا يرقى في نظر القضاء إلى درجة " الفيش " المعني بالتجريم (١).

وقد انتهى القضاء الفرنسي إلى توافر صفة " الفيش " في الدفتر الذي سجل فيه صاحب الشركة أسماء العاملين فيها وانتماءاتهم السياسية والنقابية ، بالإضافة إلى بيانات من هذا النوع تخص المرشحين للعمل بتلك الشركة(٢).

وتعتبر هذه الجريمة من الجرائم المستمرة مادام النشاط المؤثم يتمثل في وضع أو الحفاظ في ذاكرة النظام معلومات شخصية محظورة . وتنتهي الجريمة بانتهاء حالة الاستمرار . وبالتالي لا تبدأ مدة التقادم في الاحتساب إلاّ من تخلي المتهم عن هذه البيانات(٣).

(1) Crim. 3 nov. 2987, comm. J. Frayssinet in Lamy, Droit de l'informatique, mise à jour 1988.
(2) Trib. Gr. Inst. De Créteil 10 juillet 1987, D. 1988. J. 319.
(3) Crim. 4 mars 1997, op. cit.

خامسا - معالجة معلومات طبية بغرض البحث العلمي دون اتباع الطرق القانونية المقررة:

٨٠ - خصّ قانون العقوبات الفرنسي المعلومات ذات الطابع الطبي بغرض البحث الطبي بتجريم خاص بحيث يعاقب من يقوم ببرمجة معلومات من هذا النوع دون إخطار صاحب الشأن مسبقا بحقه في الاعتراض والتصحيح بعقوبة الحبس الذي لا يزيد على ٥ سنوات والغرامة التي لا تزيد على ٢٠٠ألف فرنك. كما يعاقب بنفس العقوبة من يقوم ببرمجة هذه المعلومات على الرغم من معارضة صاحب الشأن ، إذا كان من حق هذا الأخير إبداء تلك المعارضة.

خامسا - تجميع معلومات شخصية بطريقة تدليسية أو غير مشروعة:

٨١ - يعاقب قانون العقوبات الفرنسي على تجميع معلومات شخصية بطريقة تدليسية أو باتباع أي أسلوب غير قانوني . وقد قررت المادة ٢٢٦-١٨ عقوبات فرنسي عقوبة الحبس الذي لا يزيد على خمس سنوات والغرامة التي لا تزيد على ٢ مليون فرنك.

ولا تقوم الجريمة المشار إليها في البند " خامسا " إلاّ إذا تم تسجيل البيانات بعد جمعها والاحتفاظ بها في فيش أو معالجتها بالكمبيوتر [1] .

سادسا - إساءة استعمال المعلومات الشخصية:

٨٢- من الطبيعي أن يجرم القانون إساءة استعمال المعلومات الشخصية ممن يحوز هذه المعلومات. فتنص المادة ٢٢٦- ٢١ من قانون العقوبات الفرنسي على عقاب كل من استعمل المعلومات الشخصية التي تتواجد في

(1) Crim 3 nov. 1987 , Bull. crim . n° 382 , rev. sc. crim. 1988. 295, obs. Delmas Saint- Hilaire. J.C.P. 1988. I. 3323 .

حوزته في غير الغرض المخصص لها بمقتضى القانون أو اللائحة أو بمقتضى الإخطار المنصوص عليه للجهة الإدارية . يستوي أن يحدث ذلك الفعل المؤثم في مرحلة تسجيل البيانات أو نقلها أو أي مرحلة أخرى من مراحل التعامل معها . والعقوبة المقررة وفقا لهذه المادة هي الحبس خمس سنوات والغرامة ٢ مليون فرنك.

سابعا – إفشاء أسرار المعلومات الشخصية :

٨٣ – يجرّم قانون العقوبات الفرنسي فعل من يقوم بإفشاء أسرار معلومات شخصية إلى الغير الذي ليس من حقه الاطلاع على هذه المعلومات إذا كان من شأن هذه المعلومات أن تمس شرف واعتبار الأفراد أو حياتهم الخاصة.

ومن الواضح أن الإفشاء نوع من إساءة استعمال المعلومات المعاقب عليها بوجه عام في المادة ٢٢٦– ٢١ من قانون العقوبات . ومع ذلك فإنه وفقا لقاعدة أن النص الخاص يقيد النص العام ، يجب إعمال نص المادة ٢٢٦– ٢٢ من قانون العقوبات في حالة الإفشاء .

ويلاحظ أن المادة ٢٢٦ – ٢٢ عقوبات فرنسي تعاقب على إفشاء المعلومات الشخصية إذا كان من شأن ذلك أن يمس سمعة واعتبار صاحب الشأن وأن المادة ٢٢٦ – ١٣ عقوبات فرنسي في شأن إفشاء أسرار المهنة تعاقب على إفشاء معلومات قد تتماثل مع النوع الأول من المعلومات . فقد تستعين بعض الإدارات – كالضرائب والشئون الاجتماعية والسوابق القضائية – بأجهزة الكمبيوتر لتسجيل بيانات شخصية للأفراد ، و يعتبر موظفوها من الأمناء على هذه الأسرار . فإذا قام أحد منهم بإفشاء هذه الأسرار المبرمجة فإن الأمر يتعلق عندئذ بتعدد صوري للنصوص بين جريمة

إفشاء المعلومات المبرمجة (مادة ٢٢٦ – ٢٢ عقوبات فرنسي) وجريمة إفشاء أسرار المهنة (مادة ٢٢٦ – ١٣) . وحل هذا التنازع الصوري للنصوص يكون بإعمال قاعدة النص الخاص يقيد العام . فالنص الخاص بإفشاء الأسرار المبرمجة يسري على ما يعتبر من أسرار المهنة وما لا يعتبر ، كما يسري على ما يعتبر من الأمناء على الأسرار وما لا يعتبرون منتمين إلى هذه الطائفة [١] . والحقيقة أن الأمر لا يثير صعوبة ، إذ إن المشرع قد عمد إلى النص على عقوبة مماثلة في الجريمتين ، وهي الحبس مدة لا تزيد على سنة والغرامة التي لا تزيد على ١٠٠ ألف فرنك .

تطبيقا لذلك قضي بوقوع جريمة إفشاء أسرار المهنة من مدير لشركة من شركات الإقراض (الائتمان) الذي زود مجموعة من التجار بأسماء بعض الأشخاص الذين يشكلون مخاطر من ناحية وفائهم بديونهم [٢] . فقد قضي بوقوع الجريمة على الرغم من أن التجار تقدموا بطلب الإقراض لحساب المجني عليه بناء على طلب هذا الأخير . فقد كان على مدير شركة الائتمان أن يقبل أو أن يرفض هذا الطلب ولا يقوم بتزويدهم بقائمة تضم أسماء أشخاص المدينين السيئين . وذلك من شأنه أن يؤثر على سمعتهم في السوق باعتبارهم من التجار . في هذه الحالة يتوافر التنازع الظاهري للنصوص بين جريمة إفشاء أسرار المهنة وجريمة إفشاء المعلومات الشخصية المبرمجة .

ومادامت هذه الجريمة من الجرائم العمدية ، فإنها تقوم على العلم والإرادة . فإذا انتفى القصد الجنائي لا تقوم الجريمة بوصفها العمدي . وإذا انتفى الخطأ غير العمدي ينتفي وصف التهمة غير العمدية أيضا . فإذا كانت

---

(١) د. عمر الفاروق الحسيني ، المرجع ا لسابق ، ص ٦٦ .

(2) Rennes, 13 janv. 1992, D. 1993. Somm. 54 , obs.

المعلومات الشخصية عن الفرد تتمثل في بيانات عن حالته العائلية أودعها صاحبها في إحدى الوكالات المتخصصة في التعارف بين الرجال والنساء بغرض الزواج ، وقد حدث انقسام للشركة إلى شركتين cession ، فإن وجود هذه البيانات لدى الشركة الوليدة لا يحقق الركن المادي في جريمة الإفشاء . ذلك أنها ليست من الغير . يُضاف إلى ذلك أن الاتفاق مع صاحب هذه البيانات يخول الوكالة الحق في إخبار الغير المهتم بمسألة الزواج حتى يتم التعارف بين الطرفين [1]. و بالتالي فإن رضاء صاحب البيانات الشخصية يرفع عن الفعل صفة التجريم .

ولم يكتف المشرع الفرنسي بتجريم الإفشاء العمدي ، بل إنه يعاقب على الإفشاء إذا تمّ بصفة غير عمدية .عندئذ تصبح العقوبة المقررة هي الغرامة التي لا تزيد على ٥٠ ألف فرنك . وقد علّق المشرع الدعوى الجنائية عن إفشاء أسرار تلك المعلومات – سواء تمّ الإفشاء بطريق عمدي أو بطريق غير عمدي– على تقديم شكوى من المجني عليه .

---

(1) Agen 28 fév. 1994, J.C.P.1994. IV.2209 .

المبحث الثاني

ضرورة توفير الحماية الجنائية لنظام الكمبيوتر

٨٤- ضرورة استحداث نصوص خاصة لحماية المعلومات داخل الكمبيوتر:

استشعر المشرع في دول عديدة الحاجة إلى إدخال تشريعات جديدة تحمي المعلومات داخل نظام الكمبيوتر نظرا لقصور القواعد التقليدية في قانون العقوبات عن حماية هذا النظام . من هذه النصوص ما يجّرم مجرد التداخل في نظام الكمبيوتر ، ومنها ما يجرّم إتلاف المعلومات المبرمجة ، ومنها ما يجرّم تغيير هذه المعلومات . وسوف نقوم بعرض سياسة المشرع الجنائية في تشريعات عديدة في هذا الموضوع فيما يلي من سطور .

٨٥ - المعلومات داخل الكمبيوتر جديرة بالحماية عن المعلومات الورقية:

تظهر جدارة المعلومات المبرمجة آليا بالحماية الجنائية عن المعلومات التي تحتويها الملفات الورقة من ضعف النوع الأول من المعلومات ومن أهميتها في آن واحد ؛ فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية . هذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات داخل النظام . كما أن المعلومات المعالجة آليا تتميز بالضخامة والتنوع ، ومنها ما يتعلق بالحياة الخاصة للأفراد . كل هذه الاعتبارات دعت مشرعي كثير من البلاد إلى استحداث صور من التجريم لحماية المعلومات داخل الكمبيوتر من الاطلاع عليها ، بينما لا يوجد مثيل لتلك النصوص بالنسبة للمعلومات المسجلة داخل الملفات الورقية [١] .

---

(١) انظر

.Marise Cremona , Jonathan Herring , criminal law , id, p. 234

المطلب الأول

تجريم التداخل في نظام الكمبيوتر

٨٦- الاتجاه إلى تجريم مجرد التداخل في التشريعات المختلفة:

تعاقب غالبية التشريعات الحديثة على التداخل في نظام الكمبيوتر. ويعتبر القانون السويدي لسنة ١٩٧٣ أول قانون يعاقب على التداخل في نظام الكمبيوتر المملوك للغير[١].

غير أن موقف التشريعات الحديثة تتباين في تجريم التداخل. من هذه التشريعات ما يقيد تجريم التداخل بقيد يتعلق بالركن المعنوي، فيستلزم توافر قصد خاص لدى المتهم وهو قصد التأثير في البيانات أو التأثير في نظام الكمبيوتر نفسه للعقاب على هذا التداخل. من ذلك القانون الألماني والقانون الكندي والقانون النمساوي والقانون الياباني[٢]. ومن التشريعات ما لا يعاقب على التداخل إلا إذا اتجهت نية المتهم إلى الاستيلاء على أموال للغير بطريق الغش. من ذلك قانون ولاية فرجينيا بالولايات المتحدة الأمريكية[٣]. كما أن قانون جرائم الكمبيوتر في ولاية Tennessee يعاقب على التداخل إذا اتجهت نية المتهم إلى الاستيلاء على مال للغير بطريق الغش أو إلى إتلاف البيانات أو برامج النظام...

(1) Act of 2 April 1973 (section 21).

(٢) انظر:
John T. Soma , Thomas F. Muther Jr. , Heid M.L. Brissette, Transnational extradition for computer crimes; are new treaties and laws needed ? , Harvard Journal on Legislation , vol. 34, number 2, summer 1997, p. 348.

(٣) أنظر قانون ولاية فيرجينيا في شأن جرائم الكمبيوتر والذي ينص على أن:

' any person who uses a computer without authority and with the intent to :
1 - obtain property or services by false pretenses , 2- embezzle or commit larceny

ومن التشريعات ما يقيد تجريم التداخل بتوافر عنصر في الركن المادي. وتستلزم هذه التشريعات أن يحدث التداخل المعاقب عليه في خصوص أنظمة معينة كالأجهزة الحكومية أو أجهزة المؤسسات المالية أو الأجهزة التي تحوي معلومات تتعلق بالأمن القومي أو العلاقات مع الدول الأجنبية (هذا النوع الأخير من الأجهزة عادة ما ينتمي إلى الأجهزة الحكومية ، وإن أمكن تصور وقوعه على أجهزة تخص الأفراد) . من هذه القوانين القانون الفيدرالي الأمريكي لسنة ١٩٩٤ في شأن الغش وإساءة استعمال الكمبيوتر The Computer Fraud and Abuse Act (CFAA) . وفي نفس الاتجاه تعاقب تشريعات أخرى على مجرد التداخل بغض النظر عن نية المتهم ارتكاب جريمة معينة مثل القانون الأسترالي والقانون الفنلندي والقانون الهولندي والقانون السويدي والقانون الإسرائيلي [١] .

ومن التشريعات ما تورد هذا التجريم بشكل مطلق وبالتالي فإنها تعاقب على مجرد التداخل دون استلزام قصد خاص ودون استلزام قيد معين يتعلق بالركن المادي . من هذه التشريعات قانونين لبعض الولايات الأمريكية كولاية كاليفورنيا. هذا القانون الأخير يعاقب - بوصف ذلك من الجنح -كل شخص يتداخل عمدا في نظام الكمبيوتر أو شبكة الكمبيوتر أو برنامج الكمبيوتر أو في البيانات المبرمجة مع علمه بعدم رضاء صاحب النظام عن ذلك[٢] [٣]. كما أن التشريع الفرنسي يتجه نفس الاتجاه . فتنص المادة ٣٢٣ - ١ من قانون العقوبات الفرنسي على التداخل في نظام الكمبيوتر بقولها "يعاقب على الدخول أو الاستمرار في البقاء في نظام المعلومات

---

(١) انظر
John T. Soma, Thomas F. Muther, Jr. Heidi M. L. Brissette, id, p. 348.

(2) " any person who intentionally accesses any computer system , computer network , computer program , or data , knowing that the access is prohibited by the owner or lessee " (section 502 - d - 2)

(٣) يعرف قانون عقوبات لسنة ١٩٨٥ولاية كاليفورنيا تجريما آخر يعاقب فيه على التداخل إذا تم ذلك بقصد الغش أو الابتزاز أو الاستيلاء على أموال مملوكة للغير أو أنواع معينة من المعلومات أو بقصد إتلاف أو إعاقة النظام . ويتجه قانون ولاية Connecticut ، وقانون ولاية Delaware نفس الاتجاه : انظر Ulrich Sieber, id , at 89.

المبرمجة أو جزء منه – بقصد الغش – بالحبس مدة لا تزيد على سنة والغرامة التي لا تزيد على ١٠٠ ألف فرنك "[١]. وقد شددت المادة السابقة العقوبة المقررة عن هذه الجريمة إذا ترتب على هذا التداخل محو أو تعديل في البيانات المبرمجة في الجهاز. عندئذ تصبح العقوبة الحبس مدة لا تزيد على سنتين والغرامة التي لا تزيد على ٢٠٠ ألف فرنك .

٨٧- طبيعة الجريمة: التداخل جريمة نشاط

تقع جريمة التداخل بمجرد إتيان النشاط المؤثم ، وهو هنا الدخول في النظام أو البقاء في هذا النظام بعد الدخول فيه بطريقة عرضية وغير مقصودة. وبالتالي فإن المادة ٣٢٣ – ١ من قانون العقوبات الفرنسي لا تستلزم لوقوع الجريمة أن تحدث نتيجة مادية معينة . فالجريمة إذن هي جريمة نشاط أي جريمة خطر وليست جريمة ضرر . وبناء عليه فإن الجريمة تقوم عند استعمال المتهم للنظام بدون موافقة صاحبه ، حتى وإن لم يجد في الملفات ما يبحث عنه من معلومات[٢].

ومع ذلك فإن الفقرة الثانية من المادة السابقة قد اعتبرت حدوث الضرر المتمثل في حذف أو تعديل المعلومات المتضمنة داخل النظام ظرفا مشددا في الجريمة.

ويلاحظ هنا الأهمية التي يعلقها المشرع على حماية نظام المعلومات بالكمبيوتر، الأمر الذي لم يوفره قانون العقوبات للملفات الورقية التقليدية

---

(1) " Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende . Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système , soit une altération du fonctionnement de ce sysème , la peine est de deux ans d'emprisonnement et de 200 000 F d'amende ".

(٢) انظر

Marise Cremona , Jonathan Herring , Criminal law, Macmillan, second edition , p.235 .

التي تحتوي على معلومات من أهمية مماثلة . ويرجع السبب في ذلك إلى أن من يدخل نظام الكمبيوتر غالبا ما يكون قد أخلّ بحرمة المكان دون أن يقوم بدخول هذا المكان في حالات كثيرة . يضاف إلى ذلك أن نظام الكمبيوتر يتيح التعرف على كمية هائلة من المعلومات بسهولة ويسر وفي وقت قصير ، الأمر الذي لا يتوافر في حالة الملفات الورقية التقليدية .

٨٨- الركن المادي في جريمة التداخل:

يتمثل الركن المادي في جريمة التداخل في القيام بنشاط من النشاطين التاليين:

النشاط الأول : الدخول إلى النظام

النشاط الثاني : البقاء في النظام

٨٩- النشاط الأول : الدخول في النظام

٩٠- المقصود بالدخول:

يتمثل هذا النشاط في الاتصال بنظام الكمبيوتر بأي طريقة كانت . وعادة ما يقصد الفاعل بذلك الاطلاع على المعلومات التي يحتويها هذا النظام .

وقد جرّم قانون جرائم الكمبيوتر في ولاية Tenessee الأمريكية التداخل بقوله " كل من يتداخل أو يسبب تداخل الغير أو يحاول التداخل - مع علمه بذلك - في برامج الكمبيوتر أو البيانات التي يحتويها أو في نظام الكمبيوتر أو شبكة الكمبيوتر أو أي جزء مما سبق ذكره بقصد الحصول على نقود أو أموال أو خدمات لنفسه أو للغير بالاستعانة بإدعاء كاذب أو انتحال شخصية الغير أو بوعود كاذبة يعاقب بالعقوبات المقررة في فصل ٣٩ - ١٤ - ١٠٥ " . كما أورد نفس القانون التداخل بدون قصد خاص بنصه على

عقاب " كل من يتداخل أو يغير أو يتلف أو يحاول إتلاف نظام الكمبيوتر أو شبكة كمبيوتر أو برامج أو بيانات بالكمبيوتر "[١].

وقد عُني قانون ولاية Tennessee سابق الذكر بتعريف التداخل بقوله أنه "يعني كل وسيلة للاطلاع أو لإعطاء تعليمات أو للاتصال أو لتخزين بيانات أو لاستعادة بيانات أو التقاط بيانات من نظام كمبيوتر أو شبكة كمبيوتر "[٢]. ولم يخرج قانون ولاية تكساس لسنة ١٩٨٥ المعدل في سنة ١٩٩٢ عن هذا المفهوم ، حيث أورد اعتراض " التقاط " الرسائل ضمن التداخل[٣] .

٩١- المقصود بالنظام في جريمة التداخل:

يقصد بالنظام هنا نظام الكمبيوتر[٤] . ويستوي في ذلك النظام أن يكون محميا بأسلوب معين - مثل كلمة السر - أو غير محمي ، وذلك في غالبية التشريعات المقارنة مثل القانون الإنجليزي[٥] القانون الكندي[٦] والقانون

---

(١) انظر قانون ولاية Tennessee :

(b) Whoever intentionally and without authorization, directly or indirectly, : (1) accesses, or (2) alters, damages, destroys , or attempts to destroy , any computer, computer system ,computer network , computer software , program or data, violates this subsection .

(٢) انظر قانون ولاية Tennessee في شأن جرائم الكمبيوتر :

" Access" means to approach , instruct , communicate with , store data in, retrieve or intercept data from , or otherwise make use of any resources of a computer, computer system , or computer network "

(٣) انظر قانون ولاية تكساس لجرائم الكمبيوتر : § ١٠١ , ٣٣ .

definitions : (1) " Access means to approach , instruct, communicate with , store data in, retrieve or intercept data from , alter data or computer software in, or otherwise make use of any resource of a computer , computer network , computer program , or computer system. "

(٤) انظر سابقا في تعريف الكمبيوتر رقم ٢ .

(٥) انظر

Martin Wasik , Computer Crimes and Other Crimes against Information Technology in the United Kingdom , Rev.int. dr. pén. 1993, p. 632.

(٦) انظر

Donald Piragoff , Computer Crimes and Other Crimes against Information Technology in Canada , Rev.int.dr.pén.1993, p. 217.

الفرنسي . وهذا ما تتجه إليه القوانين المقارنة [1] . كما يشمل التداخل اعتراض الاتصالات بين جهازين للكمبيوتر أو أكثر من خلال الشبكات التي تربط بين تلك الأجهزة . ويمتد التداخل ليسري على صندوق البريد الإلكتروني e- mail المتواجد بالجهاز . وبديهي أن هذا التداخل لا يسري على شبكة الإنترنت نفسها ، حتى ولو تم ذلك دول الحصول على اشتراك تقديم خدمات تلك الشبكة.

٩٢- عدم الرضاء عنصر في الدخول المؤثم :

تقع الجريمة على حق من حقوق صاحب النظام على المعلومات. فالجريمة من جرائم الأموال . لذا فإنها تقع اعتداء على رضاء المجني عليه. فمادام هذا الأخير قد أبان عن عدم رضائه بدخول شخص الغير إلى نظام الكمبيوتر الذي ينتمي إليه ، فإن الدخول إلى هذا النظام دون موافقته تتحقق به الجريمة ، مادام الركن المعنوي في الجريمة قد توافر . ويعتبر عنصر عدم الرضاء متوافرا إذا علّق صاحب النظام استخدام ذلك النظام على دفع اشتراك مالي معين نظير الاستفادة من الدخول إلى هذا النظام . فتقع الجريمة ممن يقوم بالدخول إلى هذا النظام دون تسديد المقابل المالي الذي حدده صاحب النظام نظير هذه الخدمة . وبناء عليه أيضا فإن الجريمة تقوم مادام الدخول بدون رضاء قد تحقق حتى ولو لم يقم المتهم بإحاطة النظام بوسائل خاصة لحمايته من دخول الغرباء إليه [2]. يكفي إذن أن يكون قد عبّر عن رغبته في عدم السماح للآخرين بالدخول.

٩٣ - عدم تجريم الدخول وفقا للقواعد العامة :

يعتبر هذا النص تكملة للقواعد العامة التي تقضي بعدم اعتبار الحصول على المعلومات جريمة إلاّ إذا تعلق الأمر بأسرار عسكرية . فتنص

---

(١) د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، المرجع السابق ، ص ٢٩٣ .

(2) Paris 5 avr. 1994, D. 1994, D. 1994. IR. 130 .

المادة ٨٠ من قانون العقوبات مصري على عقاب من " توصل بأية طريقة إلى الحصول على سر من هذه الأسرار (يقصد الأسرار العسكرية) بقصد تسليمه أو إفشائه لدولة أجنبية أو لأحد ممن يعلمون لمصلحتها ... ". كما تعاقب المادة ٨٠ – أ عقوبات مصري " كل من حصل بأية وسيلة غير مشروعة على سر من أسرار الدفاع عن البلاد ولم يقصد تسليمه أو إفشائه لدولة أجنبية أو لأحد ممن يعلمون لمصلحتها ."(فقرة أولى) . كما تعاقب الفقرة الثالثة " كل من نظّم أو استعمل أية وسيلة من وسائل التراسل بقصد الحصول على سر من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته ". ويبقى الفارق بين النشاط المعاقب عليه في جريمة التداخل وبين جريمة الحصول على أسرار عسكرية أنه لا يلزم في المعلومات التي يحتويها نظام الكمبيوتر أن تكون ذات طابع سري .

كما نلاحظ أهمية إيراد مثل هذا التجريم ، إذا تذكرنا أن نظام الكمبيوتر لا يعتبر مسكنا في القانون وبالتالي لا يتمتع بالحماية المقررة للمسكن التي يقدمها قانون العقوبات وفقا للمادة ٣٧٠ منه . هذه المادة تنص على أن " كل من دخل بيتا مسكونا أو معدا للسكن أو في أحد ملحقاته أو سفينة مسكونة أو في محل معد لحفظ المال وكانت هذه الأشياء في حيازة آخر قاصدا من ذلك منع حيازته بالقوة أو ارتكاب جريمة فيها أو كان قد دخلها بوجه قانوني وبقى فيها بقصد ارتكاب شيء مما ذكر ، يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تجاوز ثلاثمائة جنيه مصري " . وبالمثل فإن المادة ٢٥٥ من قانون الجزاء الكويتي تنص على أن " كل من دخل مكانا مسكونا أو معدا للسكنى دون رضاء حائزه قاصدا منع حيازته بالقوة أو ارتكاب جريمة فيه يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا

تجاوز ألفي روبية أو بإحدى هاتين العقوبتين ... " .

كما لا يعتبر نظام الكمبيوتر عقارا . لذا لا يتمتع صاحب النظام بالحماية الجنائية المقررة في المادة ٣٦٩ من قانون العقوبات . هذه المادة الأخيرة تنص على أن " كل من دخل عقارا في حيازة آخر بقصد منع حيازته بالقوة أو بقصد ارتكاب جريمة فيه أو كان قد دخله بوجه قانوني وبقي فيه بقصد ارتكاب شيء مما ذكر يعاقب بالحبس مدة لا تتجاوز سنة أو بغرامة لا تجاوز ثلاثمائة جنيه مصري ... " . وبالمثل تنص المادة ٢٥٤ من قانون الجزاء الكويتي على أن " كل من دخل عقارا في حيازة آخر قاصدا منع حيازته بالقوة أو ارتكاب جريمة فيه يُعاقب بالحبس مدة لا تجاوز ستة شهور وبغرامة لا تجاوز خمسمائة روبية أو بإحدى هاتين العقوبتين ... " .

٩٤ - اختلاف التداخل عن اعتراض الرسائل المرسلة بطريق الكمبيوتر :

يختلف اعتراض الرسائل المكتوبة والتي تُرسل بطريق الكمبيوتر سواء بين جهازين عن طريق شبكة مغلقة أو بطريق الإنترنت عن التداخل . فالاعتراض لا يتضمن تداخلا في نظام معين ينتمي إلى كمبيوتر معين ، ولكنه يتمثل في التلصص على الرسائل المكتوبة المرسلة بين جهازين من الأجهزة وذلك في المسافة بين الجهاز الأول والجهاز الثاني. وهذا ما تستقر عليه تشريعات مقارنة مثل القانون الإنجليزي[1] والقانون الإسرائيلي[2]. وقد يتم ذلك عن طريق وضع وسائل سلكية تتصل بالنظام أو بطريق التقاط

---

(١) انظر

Martin Wasik, Computer Crimes and Other Crimes against Information Technology in the United Kingdom , Rev.int.dr.pén.1993,p.632.

(٢) انظر

Eli Lederman , Computer Crimes and Other Crimes against Information Technology in Israel , Rev.int.dr.pén.1993,p.404.

الرسائل بوسائل التقاط حديثة وذلك عن بعد[١]. وما دام هذا التلصص لا يتمثل في التداخل في نظام كمبيوتر معين فهو إذن لا يدخل في عداد النشاط الذي تعاقب عليه بعض القوانين بوصفه تداخلا . كما أنه لا يعتبر معاقبا عليه بوصف التنصت على المحادثات التي تجري في مكان خاص والذي تعرفه غالبية القوانين[٢].

وقد عُني القانون الإنجليزي بتعريف التداخل المؤثم بقوله في (الفصل الأول من قانون سنة ١٩٩٠) " يُسأل عن جريمة التداخل Basic Hacking Offence كل من تسبب في أن يؤدي جهاز الكمبيوتر وظيفة من وظائفه بنية التوصل إلى الاطلاع على برامج أو معلومات بداخله "[٣]

وتعاقب المادة ٣٠٩ مكررا عقوبات مصري – على التسجيل أو النقل عن طريق جهاز من الأجهزة، لمحادثات جرت في مكان خاص أو عن طريق التليفون . ويبدو من ظاهر النص أنه لا يسري على اعتراض المحادثات المكتوبة بين جهازين من أجهزة الكمبيوتر. وفي ذلك يتفق التشريع المصري مع غيره من التشريعات المقارنة ، مثل قانون العقوبات الإيطالي (617s.)

(١) انظر

Jérôme Huet Herbert Maisl, Droit de l'informatique et des télécommunications , Litec, 1989, p. 855.

(٢) انظر

Ulrich Sieber, id, p. 87 .

(3) Section 1 of the Act provides : (1) A person is guilty of an offence if : (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer , (b) the access he intends to secure is unauthorized , and (c) he knows at the time when he causes the computer to perform the function that that is the case .

وقانون العقوبات الألماني (٢٠١s.) وقانون العقوبات الهولندي (١٣٩ss. , ١٣٩-a) وقانون العقوبات السويسري (١٧٩s. bis) [١]. ويلاحظ أن تجريم التنصت لا يسري – وفقا للتشريع الكندي – إلاّ إذا كانت المحادثات بين شخصين بطريق الكمبيوتر وليس بين جهازين من أجهزة الكمبيوتر يتبادلان المراسلات المكتوبة فيما بينهما [٢] . وقد عُني المشرع الكندي بتحديد المقصود بالاعتراض بقوله " يشمل الاعتراض التنصت على أو تسجيل وظيفة من وظائف نظام الكمبيوتر " (١sub. , ٣٤٢(٢)) .

بيد أنه ليس هناك ما يحول دون أن يتسع تعبير " محادثات " الوارد في المادة السابقة لكي يشمل المحادثات المكتوبة ، بالإضافة إلى المحادثات المنطوقة . وبالتالي فإننا نرى أنه ليس هناك ما يحول دون تطبيق وصف المادة ٣٠٩ مكررا عقوبات على اعتراض المحادثات المكتوبة بين نظامين ، سواء تم ذلك عن طريق شبكة داخلية أو عن طريق شبكة الإنترنت .

وقد تنبهت بعض التشريعات إلى ضرورة إيراد نص خاص لتجريم هذه الصورة من صور النشاط ، حسما لمشكلات قانونية قد تظهر بسبب صياغة النصوص التقليدية الخاصة بالمحادثات التي تجري في مكان خاص . فيعاقب قانون العقوبات في كندا على تسجيل wiretapping المحادثات التي تتم بطريق الكمبيوتر [٣] . فيعاقب قانون العقوبات في كندا " كل من يعترض أو يتسبب في اعتراض ، بدون وجه حق وبسوء نية ، بأي طريقة

---

(١) انظر

Donald Piragoff , Computer Crimes and Other Crimes against Information Technology in Canada , Rev.int.dr.pén.1993, p. 217.

(٢)انظر

Donald Piragoff, id , p. 218 .

(٣) انظر section١٧٨ .١١ من قانون العقوبات الكندي .

كانت إلكترونية أو ميكانيكية أو سمعية أو غيرها ، بشكل مباشر أو غير مباشر ، أي وظيفة من وظائف الكمبيوتر " [1][2]. وقد عُني قانون جرائم الكمبيوتر في ولاية Tennessee الأمريكية بتعريف معنى التداخل بحيث يشكل اعتراض البيانات " intercept data "[3].

٩٥ - اختلاف التداخل في النظام عن استعماله :

تختلف فكرة التداخل عن استعمال النظام . وبالتالي فإن المشرع إذا جرّم التداخل فإن ذلك لا يعني تجريمه للاستعمال . فدائرة التداخل أضيق من دائرة الاستعمال . فكل استعمال للنظام دون رضاء صاحبه يشكل تداخلا بلا ريب فيه . أما التداخل ، فإنه لا يعني بالضرورة استعمال النظام . فقد يتصل الشخص بالنظام ومن ثم يكون متداخلا فيه ولكنه لا يستعمل إمكانيات النظام، كأن يكتفي بالاطلاع على النظام بوسائل سلكية (أي اتصال بدوائر سلكية تتصل بالنظام) أو بوسائل غير سلكية . والفاعل يكتفي عندئذ بالاطلاع دون استعمال النظام.

لذلك حرصت بعض التشريعات مثل التشريع الكندي على تجريم

---

(1) " anyone who, fraudulently and without coulour of rihgt ... by means of an electromagnetic, acoustic , mechanical or other device , intercept or causes to be intercepted , directly or indirectly , any function of a computer system " .

(٢) انظر :

Cole Durham , The Emerging Structures of Criminal Information Law: Tracing the Contours of a new Paradigm , General Report for the AIDP-Colloquium, Delits informatiques et autres infractions à la technologie de l'information , Colloque préparatoire , Wurzbourg , Allemagne , Rev. Internationale de Droit pénal ,p. 100.

(٣) انظر تعريف كلمة " access " في قانون جرائم الكمبيوتر في ولاية " Tennesse " الأمريكية :

" Access means to approach, instruct, communicate with , store data in, retrieve or intercept data from , or otherwise make use of any resources of a computer, computer system , or computer network " .

استعمال النظام بدون رضاء صاحبه . فينص التشريع الكندي على عقاب "كل من ، بسوء نية ، وبدون وجه حق : أ - يحصل ، بطريق مباشر أو بطريق غير مباشر ، على خدمة من خدمات الكمبيوتر . .... جـ - يستعمل أو يتسبب في استعمال ، بطريق مباشر أو بطريق غير مباشر ، نظام الكمبيوتر ، بنية ارتكاب جريمة من المشار إليها في الفقرة (أ) أو الفقرة (ب) أو جريمة من المشار إليها في الفصل ٤٣٠ إذا تعلق الأمر بالمعلومات المبرمجة أو نظام الكمبيوتر "(١).

٩٦- وسائل الدخول في النظام:

لا عبرة بالوسيلة التي اتبعها المتهم في الدخول إلى النظام (٢) . من الوسائل التي يمكن أن يتبعها المتهم في ذلك الآتي:

(أ) تشغيل كمبيوتر مقفول:

تتمثل هذه الطريقة في أن المتهم يقوم بفتح جهاز الكمبيوتر وتشغيله بعد أن كان مغلقا . فإذا ما بدأ العمل فإن المتهم يعتبر قد دخل النظام بدون وجه حق ، طالما تمّ ذلك دون موافقة صاحب الحق في ذلك.

ونرى أن العبرة ليس هي بتشغيل الجهاز ولكن بالتمكن من الدخول إلى الملفات ، إذ قد يتمكن المتهم من تشغيل الجهاز ، وذلك بإيصال الكهرباء

---

(١) ينص الفصل ١/٣٤٢ من قانون العقوبات الكندي على أن :

(1) Every one who fraudulently and without color of right ,
(a) obtains , directly or indirectly any computer service
(b) by means of an electro-magnetic, accoustic , mechanical or other service intercepts or causes to be intercepted , directly or indirectly , any function of a computer system , or
(c) uses or causes to be used , directly or indirectly , a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system .

(2) Paris 5 avr. 1994 , D . 1994 , IR. 130 ; comp. Douai 7 oct. 1992, Gaz. Pal.1993 .2.326, note Latry – Bonnart.

إليه، دون أن يتمكن من الدخول إلى الملفات . عندئذ يعتبر نظام المعلومات المبرمجة مقفلا على الرغم من أن الجهاز في وضع " on " .

أما إذا كان الجهاز يعمل بالفعل أي مفتوحا على ملف به معلومات ظاهرة على الشاشة ، فإن مجرد الاطلاع على تلك المعلومات - دون تحريك لائحة المفاتيح - لا يتوافر به التداخل المؤثم قانونا[١].

والتداخل المعاقب عليه لا يتوافر في حالة رضاء صاحب النظام أن يقوم المستخدم باستعمال الكمبيوتر. وبالتالي فإن عدم الرضاء ركن في هذه الجريمة . فإذا تحقق الرضاء انتفى النشاط ولم يتوافر للجريمة أركانها ، حتى ولو قام مستعمل النظام باستخدامه في غير الأغراض التي ارتضاها صاحب ذلك النظام[٢].

(ب) الدخول إلى كمبيوتر عن طريق خط تليفوني :

قد يتمكن المتهم من الوصول إلى نظام الكمبيوتر عن طريق العبث بالخط التليفوني المربوط عليه هذا النظام ، فيمكنه هذا من الاتصال بنظام من أنظمة الكمبيوتر [٣] . وعادة ما يقوم المتهم بذلك بغية التوصل إلى إعطاء أوامر لنظام الكمبيوتر لتحقيق غاية معينة . وقد كان ذلك هو شأن المتهمين الذين يعملون في شركة التليفونات الفرنسية والذين استعملوا خط التليفون المركب عليه أجهزة عارضة للألعاب الإلكترونية وتمكنوا بذلك من الحصول

---

(١) انظر
Marise Cremona , Johnathan Herring , Criminal law , id , p. 234 .

(٢) انظر
Marise Cremona , Johnathan Herring , Criminal law , id , p. 234 .

(٣) د. محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ١٩٩٤ ،

على جوائز تقدمها الشركة لمن يفوز في هذه الألعاب [1] . وواضح أن الوسيلة التي اتبعها الفاعلون كانت غير مشروعة ، كما أنهم تمكنوا من الحصول بدون وجه حق على جوائز على اعتبار أنهم فازوا في الألعاب التي قاموا بها ، بينما هم لم يفوزوا إلاّ بسبب حصولهم على ألعاب لم يدفعوا عنها المقابل المالي لكل لعبة.

(ح) الدخول إلى كمبيوتر من كمبيوتر آخر:

قد يتمكن المتهم – وهو يستعمل جهاز الكمبيوتر بطريقة قانونية – أن يدخل إلى معلومات في كمبيوتر آخر ، على الرغم من عدم وجود دائرة مشتركة بين الجهازين . ويحدث ذلك باستعمال وسائل مختلفة ، منها إجراء توصيلة بدون موافقة صاحب الجهاز الثاني، ومنها التجسس عن بعد باستعمال وسائل تقنية حديثة ودون إجراء أية توصيلات.

وقد يتمكن المتهم من الدخول إلى نظام آخر من أنظمة الكمبيوتر بالاتصال عن بعد بهذا النظام والتوصل إلى معرفة كلمة السر والدخول إلى النظام كله أو جزء منه . كل ذلك يتحقق به الفعل المعاقب عليه.

ومن التطبيقات على هذه الصورة من صور النشاط الإجرامي أن يقوم المتهم بالتداخل في نظام كمبيوتر معين – وكان هذا النظام قد تلقي أمرا بطريقة مشروعة لتحويل مبلغ مالي إلى حساب معين – ليخدع به الكمبيوتر المتلقي لهذا الأمر ليقوم بتحويل المبلغ إلى حساب آخر [2].

وبالمثل فإن المتهم قد يقوم بالتداخل في أجهزة الكمبيوتر الخاصة بخدمة

---

(1) Aix – en – Provence, 23 oct. 1996, Gaz Pal . 1997. 2. 489, note Latry – Bonnart ; Rev. sc. crim. 1998. 140, obs Francillon .
(2) Travaux de l'Institut de sciences criminelles de Poitiers , Informatique et droit pénal , op. cit. , p. 25 .

التليفون ويتمكن من الحصول على مكالمات تليفونية مجانية [1] . ومن التداخل المؤثم في النظام ما قام به المتهمون من التقاط المكالمات التليفونية التي تصل إلى إحدى محطات الإذاعة المحلية ومنعها من الوصول إلى المحطة حتى لا يشترك أصحاب هذه المكالمات في مسابقة تعدها تلك المحطة. وقد تمكن المتهمون بهذه الطريقة من أن يفوزوا في المسابقة لأنهم أصبحوا الوحيدين للاشتراك في تلك المسابقة (قضية Pelerson)[2].

(د) الدخول إلى نظام متصل بنفس الكمبيوتر :

يقوم المتهم في هذه الحالة باستعمال جهاز كمبيوتر بطريقة قانونية، فقد يكون جهازه وقد يكون جهاز شخص آخر يقوم باستعماله بموافقة منه. لكنه يستعمل هذه الجهاز في الدخول إلى أنظمة أخرى يتصل بها هذا الجهاز ويتاح له الدخول فيها ولكن نظير اشتراك مالي معين.

ويفترض هذا النشاط المعاقب عليه أن المتهم ليس من حقه الدخول في النظام . فإذا كان من حقه هذا الدخول فإن الجريمة لا تقع ، حتى ولو قام باستعمال هذا النظام في غير الغرض الذي سمح به صاحبه . تطبيقا لذلك قضي في إنجلترا (في ١٤ نوفمبر سنة ١٩٩٤) بعدم وقوع الجريمة من مستخدمي إحدى الجهات العامة العاملين بالكمبيوتر الذين اتصلوا بإحدى الصحف العامة لكي يثبتوا لهم أن أجهزة الكمبيوتر الخاصة بتلك الجهة يمكن اختراقها والاطلاع على أسرار الجمهور لدى تلك الجهة . وقاموا بإجراء تلك التجربة من خارج تلك الجهة [3] . وقد كان قانون مكافحة إساءة

---

(1) James Richards, " Transnational Criminal Organisations, Cybercrime , CRC Press , New York , Washington D. C. , 1999, p. 69 .

(2) James Richards , id, p. 70 .

(٣) مشار إليه في

" Stanley Lai , Unauthorised use and section 1of the Computer Misuse Act 1990 " , Journal of Financial Crime , May 1996, Vol.3, N° 4 , p. 359.

استعمال الكمبيوتر the Computer Misuse Act ١٩٩٠ في إنجلترا محلا للانتقاد ، لأنه لا يعاقب على إساءة استعمال الكمبيوتر ممن له حق الدخول في النظام ، مع أن عنوان القانون يدلل على أنه شُرع لمكافحة إساءة استعمال الكمبيوتر[1].

وقد حرص قانون إساءة استعمال الكمبيوتر Computer Misuse Act ١٩٩٠ على أن التداخل المعاقب عليه هو التداخل غير المصرح به unauthorised access . وقد حدد الفصل رقم ١٧ فقرة ٥ بأنه يتوافر في حالتين : أ- عندما لا يكون للشخص الحق في السيطرة على الدخول إلى البرنامج program أو البيانات data. ب – عندما لم يصرح له صاحب الحق في الدخول إلى البرنامج أو البيانات.

من ذلك أنه يجوز استعمال شبكة الإنترنت للدخول إلى عدة مواقع وذلك نظير استعمال بطاقة مدفوعة الأجر . وقد يتقيد استعمال بعض المواقع على شبكة الإنترنت بضرورة إدخال كلمة معينة للسر. ومؤدى ذلك أن صاحب هذا الموقع لا يرضى إلاّ لمن زوده بكلمة السر بالدخول إليه ومعرفة ما يحتويه هذا الموقع من بيانات . فإذا تحايل المتهم وقام بتجربة استعمال أكثر من كلمة للسر حتى دخل على هذا الموقع ، فإنه يرتكب الفعل المؤثم بمقتضى المادة ٣٢٣- ١ من قانون العقوبات الفرنسي.

(هـ) التجسس على النظام :

في هذا الفرض لا يقوم الفاعل باستعمال النظام ، ولكنه يقوم بالاطلاع على محتوى هذا النظام ، أي يقوم بالتجسس على ما به من بيانات عند تشغيله . وهناك وسائل عديدة لهذا التجسس منها وضع توصيلات بالجهاز

---

(1) Stanley Lai , id, p. 358.

بدون موافقة صاحبه ، ومنها اتباع وسائل حديثة لالتقاط المعلومات التي يحتويها الجهاز عند بعد[1]. ويحدث هذا الفرض الأخير عادة عند استعمال الجهاز وليس تركه مغلقا.

٩٧ – تجريم بعض التشريعات لمحاولة التداخل:

تعاقب بعض التشريعات على محاولة التداخل ، ولو لم يتمكن المتهم من التوصل إلى التداخل في نظام ينتمي إلى الغير . فقد يحاول المتهم استعمال كلمات عديدة للسر لكي يتمكن من التداخل في أنظمة الكمبيوتر الخاصة بالدولة أو بالمؤسسات المالية لكي يطلع على معلومات سرية في هذه الأنظمة أو يرتكب جريمة من الجرائم المالية أو يقوم بعملية تخريبية لهذه المعلومات . من هذه التشريعات القانون الأمريكي الفيدرالي لسنة ١٩٩٤ Computer Abuse Amendments Act of ١٩٩٤ [2] . هذا القانون يعاقب على محاولة استعمال كلمات السر للدخول إلى أجهزة الكمبيوتر الحكومية أو إذا وقعت هذه المحاولة بقصد التأثير على التجارة الخارجية أو التجارة بين الولايات [3]. ويعاقب القانون الأمريكي على استعمال أرقام بطاقات الائتمان أو أي رقم شخصي ينتمي إلى الغير بدون رضائه بغرض الحصول بغير حق على خدمات أو أموال[4].

---

(١) انظر :

Guillaume CHAMPY , La fraude informatique , op. cit., p. 153 .

(٢) انظر

. ((a) 5(A U.S.C.A. §

(٣) انظر

John M. Scheb , John M. Scheb II , Criminal law & procedure , West / Wadsworth, third edition , 1999, p. 235.

(٤) انظر

18 U.S.C.A. § 1029 (e) .

ومؤدى هذا الاتجاه الأخير وقوع الجريمة ليس فقط بالتداخل الفعلي في نظام ينتمي إلى الغير ولكن بمحاولة القيام بهذا التداخل عن طريق استعمال طرق معينة إذا كان غرض هذا التداخل التوصل إلى ارتكاب جرائم معينة . وبالتالي فإنه يلزم لتجريم المحاولة أن يقع باستعمال وسيلة معينة مثل كلمة السر أو أرقام بطاقات الائتمان أو أرقام اشتراك العملاء . كما يلزم في الركن المعنوي توافر قصد من نوع خاص هو التوصل إلى ارتكاب جرائم معينة كجرائم الأموال أو الإرهاب أو المخدرات.

النشاط الثاني : البقاء في النظام بعد الدخول عرضا إليه

٩٨ – يتمثل هذا النشاط في بقاء المتهم داخل نظام للكمبيوتر بعد أن يكون قد دخله عرضا وبطريق الخطأ[1]. فمجرد الدخول الخاطئ لا يعاقب عليه القانون، ولكن يعاقب على البقاء في هذا النظام بعد أن تبين المتهم جلية الأمر.

وقد يدخل المتهم النظام بطريق مشروع ، ولكنه يستمر بعد الوقت المحدد لبقائه فيه[2]. وكثيرا ما يحدث ذلك إذا كان استعمال النظام محددا بوقت معين نظير أجر مالي ، فيتخطى المتهم هذا الوقت [3] . وبالتالي يسمح هذا النص بتجريم ما يمكن أن نطلق عليه " سرقة وقت الآلة "[4].

وقد أعمل القضاء الفرنسي تجريم البقاء في النظام في قضية تتلخص

---

(1) Paris 5 avr. 1994. D. 1994. IR. 130 .

(٢) د. على عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونيا ، مؤتمر العين ، المرجع السابق ص ٥٢ .

(٣) د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، المرجع السابق ، ص ٢٩٩ .

(4) Michel VERON , Droit pénal spécial , éd. Armand Colin , 1999, p. 266 .

وقائعها في قيام بعض العاملين في شركة الخطوط التليفونية باستعمال تلك الخطوط – دون دفع المقابل المالي – للقيام بألعاب " الفيديو جيم " للحصول على جوائز مقررة لمن يستمر في اللعب مدة معينة [١] . وقد أعمل هذا القضاء وصف البقاء في النظام بطريق الغش ، وليس وصف التداخل في النظام ، حيث إن هؤلاء العاملين كان من حقهم التداخل في النظام أصلا لمراقبته والإشراف عليه وإصلاح أعطاله [٢] .

كما أنزل القضاء الفرنسي هذا الوصف على من عمد إلى إرسال رسائل وهمية إلى شركة من الشركات التي تتولى تقديم خدمات التليماتيك serverur télématiques بغرض خلق ازدحام على خطوط التليفونات التي يستعملها زبائن تلك الشركة ، إضرارا بمصالحها [٣] . كما أدى تدخل المتهمين إلى خلق ازدحام في صناديق بريدها الإلكتروني بهذه الرسائل الفارغة أو المضللة ، مما تسبب في اضطراب علاقة تلك الشركة بزبائنها. وقد قصد المتهمون إلى تحقيق تلك الغاية سعيا إلى حمل زبائن تلك الشركة إلى شركتهم التي تعمل في نفس المجال أيضا. وقد جاء انتهاء القضاء الفرنسي إلى وقوع جريمة البقاء في النظام بنية الغش وليس إلى وقوع جريمة التداخل في النظام بدون وجه حق ، استنادا إلى أن الجمهور كان من حقه أن يتداخل في النظام للاتصال بمراكز هذه الخدمات.

---

(1) Trib. corr. De Paris 5 nov. 1996, Cahiers Lamy droit de l'informatique , Bulletin d'actulité, n° 89 fév. 1997, p. 9 et 10 .

(٢) وجدير بالذكر أن المحكمة – في هذا الحكم – قد انتهت أيضا إلى وقوع جريمة النصب ، حيث إنه لا شيء يحول دون وقوع هذه الجريمة على الخدمات التي لها قيمة مالية وفقا لقانون العقوبات الفرنسي الذي دخل حيز التطبيق في سنة ١٩٩٤ . كما قضت المحكمة بتوافر جريمة إخفاء الأشياء المتحصلة من جريمة .

(3) Cour d'appel de Paris 14 janvier 1997, Cahiers Lamy droit de l'informatique, Bulletin d'actualité, n° 97, nov. 1997, p. 12.

٩٩- لحظة تمام جريمة التداخل:

تقع جريمة التداخل تامة عندما يتحقق أحد النشاطين المعاقب عليهما، وهما الدخول في النظام أو البقاء فيه.

وتقع جريمة التداخل تامة حتى ولو لم يحصل المتداخل على معلومات. فالنشاط يتمثل في التداخل في النظام، حتى ولو كان هذا النظام لا يحوى سوى معلومات غير ذات أهمية . وأكثر من ذلك فإن الجريمة تقع بمجرد التداخل حتى ولو لم يتمكن المتداخل من الاطلاع على أية معلومات. ويبرهن ذلك على أن هذه الجريمة من جرائم الخطر.

ومع أن هذه الجريمة من جرائم النشاط ، فإن الشروع فيها أمر متصور وذلك عندما يقوم المتداخل بتشغيل النظام دون أن يتمكن من الدخول في نظام البيانات نفسه. وقد يرجع ذلك إلى أن المتهم قد تمّ ضبطه بعد تشغيل الجهاز وقبل أن يتمكن من فتح أي ملف من الملفات المدوّنة بالكمبيوتر . وقد يرجع عدم تمكن المتهم من الدخول إلى الملفات على الرغم من فتح الجهاز أن يكون تشغيل الملفات معلقا على استعمال كلمة للسر . هذه الكلمة قد لا يعرفها المتهم.

١٠٠ - اختلاف جريمة التداخل عن جريمة البقاء في الطبيعة القانونية:

تختلف جريمة التداخل عن جريمة البقاء في أمرين:

الأمر الأول : إن جريمة البقاء لا تصدر من الفاعل في جريمة التداخل . ويرجع السبب في ذلك إلى أن تجريم البقاء هو من قبيل النص الاحتياطي بالنسبة لتجريم التداخل. فلا تُنسب جريمة البقاء إلى من قام بالتداخل. والأمر في ذلك يتماثل مع تجريم إخفاء الأشياء المسروقة بالنسبة لجريمة

السرقة نفسها . فالفاعل في جريمة السرقة الذي يحتفظ بالمسروقات لا يُنسب إليه أنه قام بارتكاب جريمة أخرى هي إخفاء المسروقات[1]. هـذا التجـريم الأخير يخاطب شخصا لم يساهم في جريمة السرقة ، إلى تلك النتيجـة انتهـت أحكام القضاء الفرنسي[2]. وبالمثل فإن من قـام بارتكـاب جريمـة القتـل، لا يرتكب جريمة إخفاء جثة القتيل على الرغم من قيامه بذلك . هذا الإخفـاء هو من قبيل النصوص الاحتياطيـة الـتي أُعـدت لتخاطـب غـير المساهم في القتل.

وترجع أهمية ما سبق بيانه إلى أن جريمة التداخل جريمة مؤقتة[3]، أما جريمة البقاء فإنها من طبيعة مستمرة . وبالتالي فإن التقادم تُحتسب مدته من وقت التداخل بالنسبة لمن قام بذلك التداخل ، حتى ولو استمر في البقاء في النظام ، مادام أن هذا التداخل مشكلا للجريمة . أما إذا كـان التـداخل غـير مقصود ثم علم المتهم بتداخله ففضل البقاء ، فإنه يُنسب إليه جريمة البقاء في النظام وتُحتسب مدة التقادم من الوقت الذي فيه ينتهي هذا البقاء .

١٠١- الركن المعنوي:

أفصحت المادة ٣٢٣- ١ من قانون العقوبات الفرنسي عن تطلب القصد الجنائي بقولها " بطريـق الغـش frauduleusement " . وبالتـالي فـإن هـذه الجريمة لا شك أنها من الجرائم العمدية.

---

(١) انظر :

Roger Merle , Nandré Vitu, Traité de droit criminel , droit pénal spécial,éd. Cujas 1982, p. 2001.

(2) Crim. 15 déc. 1949, Bull.crim. n° 350 ; 2 déc. 1971, Bull.crim.337.

(٣) انظر :

Guillaume CHAMPY, op. cit., p. 152 .

١٠٢- الظروف المشددة في الجريمة:

أوردت المادة ٣٢٣ – ١ عقوبات فرنسي ظرفا مشددا لهذه الجريمة يتمثل في تشديد العقوبة المقررة للتداخل إذا ترتب عليه ، إما إلغاء أو تعديل بيانات مبرمجة في النظام ، أو الإخلال بسير ذلك النظام[١]. فالعقوبة المقررة للتداخل هي الحبس مدة سنة والغرامة ١٠٠ ألف فرنك . وتشدد العقوبة عند توافر الظرف المنوه عنه إلى الحبس مدة لا تزيد على سنتين والغرامة التي لا تتجاوز ٢٠٠ ألف فرنك.

وقد أحسن المشرع الإنجليزي عندما أورد ظرفا مشددا آخر عندما يتجه قصد الفاعل إلى ارتكاب جريمة أخرى أشد من جريمة التداخل (Section ٢ of Computer Misuse Act ١٩٩٠). وليس من الضروري لتوافر هذا الظرف المشدد أن تقع الجريمة الأشد . يكفي إذن أن يتوافر قصد خاص وهو انصراف نية الفاعل إلى ارتكاب تلك الجريمة[٢]. بل إن هذا الظرف المشدد يتوافر ولو كانت الجريمة الأخرى جريمة مستحيلة[٣].

---

(1) Michel VERON, p. 266.

(٢) انظر

Marise Cremona , Jonathan Herring, id, p. 235 .

(٢) انظر

Marise Cremona , Jonathan Herring, id , p. 235.

المطلب الثاني

تجريم إعاقة نظام الكمبيوتر أو الإخلال بسيره

١٠٣- تضمنت المادة ٣٢٢- ٢ من قانون العقوبات الفرنسي هذا التجريم بنصها على أن " يعاقب على إعاقة أو الإخلال بسير نظام معالجة المعلومات بالحبس مدة لا تزيد على ٥ سنوات والغرامة التي لا تزيد على ٣٠٠ ألف فرنك "[١]. وقد تضمن القانون الإنجليزي لسنة ١٩٩٠ Computer Misuse Act نصا متشابها للعقاب على " كل تعديل لمحتوى الكمبيوتر دون إذن صاحب الحق فيه ".

وبناء عليه فإن تلك الجريمة تتشكل من ركن مادي وركن معنوي . يتمثل الركن المادي في الإعاقة أو الإخلال بنظام المعلومات ، ويتمثل الركن المعنوي في القصد الجنائي.

١٠٤- الركن المادي :

يتكون الركن المادي في جريمة الإعاقة أو الإخلال بسير النظام في أحد النشاطين التاليين :

١- الإعاقة :

- يقصد بالإعاقة منع النظام بصفة كلية أو بصفة جزئية من العمل . من صور إعاقة النظام إدخال " فيروس " يؤدي إلى وقف عمل النظام كليا أو جزئيا[٢].

---

(1) " Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 F d'amende ".

(2) Michel VERON , p. 267.

وقد ترد الإعاقة على برنامج من البرامج التي يحتويها النظام وليس على كل نظام الكمبيوتر.

٢ – الإخلال بسير النظام:

– يقوم المتهم في هذه الصورة من النشاط بإدخال ما من شأنه أن يسبب خللا في نظام عمل الكمبيوتر. فالنظام يعمل في هذه الحالة ولكن بصورة بطيئة أو بصورة مضطربة بحيث تبتعد عن الصورة المعتادة لعمل النظام . ويشمل هذا النظام كل تشويه في سير النظام بحيث يؤدي إلى نتائج غير سليمة وفقا للصورة المعتادة لعمل هذا النظام .

تطبيقا لذلك قُضي بوقوع الجريمة من المتهمين الذين دأبوا على إرسال رسائل كثيرة ، بدون وجه حق ، عبر نظام الكمبيوتر ، مما أدى إلى إرباك النظام المتلقي لهذه الرسائل والتي تمثلت في طلبات اشتراك في مسابقة من المسابقات التي يمكن أن تنتهي بالحصول على جوائز [1] .

وقد يرد الإخلال في طريقة العمل على برنامج من البرامج وليس على كل النظام .

١٠٥- الركن المعنوي:

يُثار التساؤل عن شكل الركن المعنوي أي عن مدى تطلب القصد الجنائي أو الخطأ غير العمدي لوقوع تلك الجريمة.

١٠٦- تطلب القصد الجنائي:

نصت المادة ٣٢٣- ٢ من قانون العقوبات الفرنسي على عقاب " كل من قام بتعطيل النظام أو أخلّ بسيره ... " . ولم يحدد النص شكل الركن

---

(1) Paris , 5 avr. 1994 , D. 1994, Flash , n° 18 .

المعنوي بصورة واضحة . و نزولا على قواعد التفسير التي تقضي بأنه إذا لم يحدد النص العقابي شكل الركن المعنوي ، فإن الأصل هو العقاب عن الأفعال العمدية[1]. ولا نعتقد أن المشرع أراد أن يسوي بين القصد والخطأ غير العمدي .

وبالتالي فإن تلك الجريمة من الجرائم العمدية ، وقوام الركن المعنوي فيها هو القصد الجنائي الذي يتشكل من علم وإرادة . وتستخلص محكمة الموضوع توافر القصد الجنائي من ظروف وملابسات الموضوع . فإذا قام المتهم بإدخال فيروس في شريط ممغنط ، وقد انتقل هذا الفيروس إلى الجهاز عند استعماله ، فإن ذلك يدلل بشكل واضح على توافر القصد الجنائي لدى المتهم. ذلك أن زرع فيروس في الشريط الممغنط يدل وفقا لظاهر الأمور على أن المتهم يعلم بأن الشريط سوف يستخدم في عمل الجهاز وأن الفيروس سوف ينتقل إليه. ولا يقدح في ذلك أن كثيرا من مستخدمي النظام يستخدمون برامج مضادة للفيروسات ، إذ إن عدم استخدام هذه البرامج الواقية لا ينفي توافر الركن المادي من نشاط يتمثل في زرع الفيروس ومن نتيجة تتمثل في إعاقة النظام أو الإخلال بسيره . لذا قُضي بنقض الحكم الذي انتهى إلى براءة المتهم ، استنادا إلى الشك في الأدلة ، إذا ثبت أن المتهم قد زرع فيروس في شريط ممغنط وترتب على ذلك إعاقة النظام [2] .

ولا تقوم الجريمة استنادا إلى الخطأ غير العمدي . فإذا نسب إلى المتهم أنه في أثناء تجاربه على نظام الكمبيوتر حدث إغلاق للنظام وإضاعة البيانات

(١) د. عبد الرءوف مهدي ، شرح القواعد العامة لقانون العقوبات ، ١٩٨٣ ص ٢٠٠ .

(2) Crim. 12 déc. 1996, Bull . crim. n° 465; Rev. sc. crim. 1998, obs. Francillon ; RTD com. 1997. 521; Gaz, Pal . 16 – 17 avr. 1997, cassation de Paris 15 mars 1995: J.C.P. 1995, IV. 1425 .

المبرمجة فيه ، فإن الجريمة لا تقوم رغم ذلك لانتفاء القصد الجنائي[1] .

١٠٧- حالة الاكتفاء بالقصد المتعدي:

يُعاقب على التداخل العمدي إذا ترتب عليه الإخلال بنظام سير الجهاز بطريق القصد المتعدي ، باعتبار أن المتهم لم يقصد إلى تحقيق ذلك الإخلال ولكنه محتمل لفعل التداخل . ويُصاغ هذا التجريم على غرار الضرب المفضي إلى موت. وبديهي أنه إذا انصرف قصد المتهم بتداخله إلى تحقيق ذلك الإخلال ، فإن جريمة أخرى عمدية هي التي تقع . فتنص المادة ٣٢٣-١ من قانون العقوبات الفرنسي على العقاب على التداخل في النظام أو البقاء فيه بطريق الغش بالحبس مدة سنة والغرامة التي لا تزيد على ١٠٠ ألف فرنك . وتشدد العقوبة إلى سنتين حبس ، بالإضافة إلى الغرامة التي لا تزيد على ٢٠٠ ألف فرنك ،إذا ترتب على هذا التداخل أو ذلك البقاء في النظام الإخلال نظام سير ذلك النظام.

(1) Corr. Poitiers , 26 juin 1997; Gaz. Pal . 1997, chron. 215, Rev. sc. crim. 1998, 145.

المطلب الثالث

تجريم العبث بالبيانات المبرمجة

١٠٨ - يقصد بالعبث بالبيانات المبرمجة إدخال بيانات غير مصرح بها في النظام أو تعديل بيانات موجودة أو إلغاء هذه البيانات [1]. فتنص المادة ٣٢٣ - ٣ من قانون العقوبات الفرنسي على عقاب كل من أدخل ، بسوء نية ، بيانات في نظام معالجة البيانات أو قام - بسوء نية - بإلغاء أو تعديل هذه البيانات بالحبس مدة لا تزيد على ثلاث سنوات حبس والغرامة التي لا تزيد على ٣٠٠ ألف فرنك.

يبين مما سبق أن تلك الجريمة تقوم على ركنين : ركن مادي وركن معنوي.

١٠٩- الركن المادي:

يقوم الركن المادي على النشاط في الجريمة . فالجريمة من جرائم النشاط التي لا يلزم لتحققها حدوث نتيجة مادية معينة . ويتمثل النشاط في توافر إحدى صور النشاط التالية :

- إدخال بيانات غير مصرح بها
- تعديل بيانات قائمة
- إلغاء بيانات قائمة

وبناء عليه فإن الركن المادي في هذه الجريمة يقوم على تعديل المحتوى المادي للبيانات المبرمجة . هذا التعديل قد يتخذ صورة الإضافة أو الحذف أو

---

(١) انظر د. سامي الشوا ، المرجع السابق ، ص ٨٣ .

تغيير البيانات ذاتها[1]. وقد أدخل المشرع الفرنسي هذا التجريم لأن القواعد العامة في تزوير المحررات غير ملائمة لمكافحة تلك الصورة من صور العبث بالبيانات . وقد سبق أن أوردنا الأسباب التي تقف وراء صعوبة إعمال القواعد العامة في تزوير المحررات على تعديل البيانات المبرمجة . من أهم هذه الأسباب عدم توافر شرط المحرر في البيانات المبرمجة[2].

وقد أحسن المشرع الفرنسي صنعا عندما أدخل هذا النوع من التجريم لكي يحمي البيانات المبرمجة . هذه البيانات قد تم برمجتها في الكمبيوتر حتى تحل محل البيانات المكتوبة في الملفات الورقية في شكلها التقليدي . ومن المعروف أن هذه الملفات تصلح أن تكون محررات مادام أنه يمكن التمسك بها في ترتيب آثار قانونية . عندئذ يعتبر العبث بها مشكلا لجريمة التزوير في أوراق عرفية أو في أوراق رسمية ، بحسب ما إذا تعلق الأمر بمحررات رسمية أو بمحررات عرفية . بيد أنه يلاحظ أن بعض الأوراق الموجودة بالملفات الورقية لا تشكل محررات لأنها لا تصلح للاحتجاج بها ، وإنما أعدت للاستعمال الداخلي . في هذه الحالة لا يكون التعديل فيها مشكلا لجريمة التزوير في المحررات . عندئذ لا يبقى سوى جريمة الإتلاف إذا وصل هذا التعديل إلى درجة إتلاف المستند . وهنا تظهر أهمية جريمة العبث بالبيانات المبرمجة . فهي تحقق للبيانات داخل الكمبيوتر حماية أكثر من تلك التي توفرها القواعد العامة في تزوير المحررات للمحررات الورقية. ذلك أن تلك الحماية تنسحب على كافة البيانات ذات القيمة ولو لم تكن من شأنها أن ترتب آثار قانونية .

ومن التطبيقات القضائية على جريمة إدخال بيانات غير مصرح بها ما قامت به المتهمة التي كانت تعمل في إحدى الشركات ، وذلك قبل تركها العمل في تلك الشركة من إدخال بيانات غير صحيحة تتعلق بمعدل احتساب

(1) Crim 5 janv. 1994, Gaz. Pal . 1996. somm. 419; 12 déc. 1996, Bull. crim. n° 465.

(2) انظر ما سبق رقم ١٦٥

الضريبة على القيم المنقولة[1]. وقد أدى ذلك إلى إرباك العمل بما كانت تزمع الشركة القيام به من أعمال المحاسبة داخل الشركة . ومن الواضح أن قصد المتهمة كان منصرفا إلى تحقيق تلك الغاية.

ويلاحظ أن هذه الجريمة وهي تعديل البيانات تختلف عن جريمة أخرى وهي إعاقة أو الإخلال بسير النظام ، على الرغم من أن تلك الجريمة الأخيرة يمكن أن تقع بتعديل المتهم للبيانات . بيد أن ثمة فارقا بين الاثنين يتمثل في أن تعديل البيانات أو إدخال بيانات كاذبة ليس من شأنه أن يؤدي دائما إلى إعاقة النظام أو الإخلال بسيره الطبيعي دائما.

١١٠- الركن المعنوي :

تلك الجريمة من الجرائم العمدية التي تقوم على القصد الجنائي ، ذلك أنها من الجرائم العمدية . ويرجع ذلك إلى صياغة المادة ٣٢٣ - ٣ من قانون العقوبات الفرنسي التي استخدمت تعبير " بسوء نية ".

ومع ذلك فإن قانون العقوبات الفرنسي يعاقب على تعديل البيانات أو محوها إذا تمّ ذلك بطريق الخطأ ، أي دون توافر قصد التغيير أو الحذف ، وفقا للمادة ٣٢٣ - ١ عقوبات . ويتوافر هذا الفرض في حالة جريمة التداخل أو البقاء في النظام بطريق الغش إذا ترتب على ذلك تعديل البيانات الموجودة في النظام أو محوها . هذا التعديل أو ذلك الحذف يعتبر سببا في تشديد العقاب في جريمة التداخل أو البقاء ، وتصبح العقوبة المقررة هي الحبس مدة سنتين والغرامة ٢٠٠ ألف فرنك . أما إذا لم يترتب على التداخل حدوث أي تعديل أو حذف للبيانات أو حدوث إخلال بسير عمل النظام نفسه ، فإن العقوبة لا تكون إلاّ الحبس مدة سنة واحدة والغرامة ١٠٠ ألف فرنك .

(1) Cass. crim. 5 janv.1994, J.C.P. 1994. I. 359 , obs. Vivant et Le Stanc.

المبحث الثالث

ضرورة الأخذ في الاعتبار الوضع الخاص باستعمال الإنترنت في ارتكاب الجرائم

١١١- على الرغم من الفائدة العظيمة لشبكة الإنترنت في تسهيل الاتصال عبر الدول ، سواء بين الأفراد أو بين الشركات ، فإن ظهور تلك الشبكة كان وسيلة استعان بها بعض المجرمين لارتكاب جرائم متنوعة ، منها ما يتعلق بالأموال ومنها ما يتعلق بالمصلحة العامة .

لذا كان لزاما على المشرع أن يواجه ذلك الوضع الجديد المرتبط بسهولة استعمال شبكة الإنترنت في ارتكاب الجرائم وذلك باستحداث نصوص جديدة تعاقب على أفعال جديدة أو تشدد العقوبة على أفعال معاقب عليها أصلا .

وعلى المشرع عند استحداثه للنصوص الجديدة أن يأخذ في اعتباره الطبيعة الخاصة للاتصال عبر شبكة الإنترنت والتي تتجلى في العناصر التالية:

١ – إن شبكة الإنترنت تستعمل كوسيلة لارتكاب بعض الجرائم

٢ – إن شبكة الإنترنت تحقق ركن العلانية الذي يتطلبه القانون لوقوع بعض الجرائم .

٣ – إن شبكة الإنترنت تحقق البعد الدولي للجرائم التي تقع بواسطتها .

المطلب الأول

استخدام شبكة الإنترنت في ارتكاب الجرائم

١١٢- تتميز شبكة الإنترنت بتسهيل ارتكاب كثير من الجرائم ، منها جرائم الأموال وجرائم الإرهاب والاتجار في المخدرات وغسيل الأموال غير المشروعة . هذا التسهيل يستدعي تدخلا من المشرع لتشديد العقاب ليواجه بها السهولة التي يتم بها ارتكاب الجريمة.

١١٣- استعمال شبكة الإنترنت في ارتكاب جرائم الأموال:

يستعمل بعض المجرمين شبكة الإنترنت في ارتكاب جرائم الأموال مثل السرقة و خيانة الأمانة و النصب.

(أ) استعمال شبكة الإنترنت في ارتكاب خيانة الأمانة:

١١٤- قد تقع جريمة خيانة الأمانة في التعاملات المالية التي تتم بطريق الإنترنت عندما يرسل العميل رقم حسابه إلى المتعامل معه في صفقة تجارية أو في أي صورة من صور التعاملات المالية ، على أن يقوم هذا الأخير باستعمال رقم الحساب في سحب مبلغ معين من حساب العميل من البنك ، فيقوم الطرف الثاني بسحب مبلغ أكبر من المتفق عليه .

في هذا الفرض يقوم المتهم باستعمال رقم الحساب الذي عهد به صاحبه إليه أي الذي أرسله إليه صاحبه على وجه الأمانة . ولما كان هذا الرقم عندما يكون مكتوبا على دعامة مادية وهي شبكة الإنترنت يعد مالا ، ولما كان ذلك يتضمن تسليما لهذا المال على سبيل الأمانة ، ولما كان نشاط المتهم يشكل الركن المادي في جريمة خيانة الأمانة ، فإن قيامه بسحب المبلغ

الزائد يجعله مسئولا عن جريمة خيانة الأمانة . ولا ريب أن المتهم قام بالنشاط الإجرامي في خيانة الأمانة وهو سحبه من الرصيد مبلغا يزيد عن المتفق عليه ، كمن أؤتمن على مفتاح مخزن به بضاعة ليقوم بصرف البضاعة المتفق عليها ، فيقوم بصرف ما يزيد على المتفق عليه . ويؤدي هذا إلى القول بأن المال محل الأمانة هو الموجود بحساب العميل ، وقد قام المتهم بالسحب من هذا المال بالمخالفة للالتزام بالأمانة بمقتضى عقد من عقود الأمانة وهو عقد الوكالة . غير أنه لا يخفى أيضا أن رقم الحساب هو نفسه مال كان محلا للتسليم على سبيل الأمانة من صاحب الحساب . وقد اتخذ التسليم صورة الإرسال عبر شبكة الإنترنت. وقد تمثل سلوك المتهم في استعمال هذا الرقم بطريقة مخالفة لواجب الأمانة . هذا الاستعمال يتضمن الظهور على الشيء بمظهر المالك، ومن ثمّ يتوافر فيه النشاط المعاقب عليه في خيانة الأمانة عند استعماله في الصرف من الحساب لمبلغ أكبر من المتفق عليه .

(ب) استعمال الإنترنت في ارتكاب جرائم النصب:

١١٥- قد تتيح شبكة الإنترنت ارتكاب جريمة النصب ، كمن يقوم بالاطلاع على رقم حساب أحد العملاء الذي يرسله إلى المتعامل معه ويقوم باستعماله في سحب مبلغ مالي من حساب هذا العميل.

يمكن القول بأن قيام المتهم بالاطلاع على رقم الحساب عن طريق شبكة الإنترنت لا يشكل اختلاسا لهذا الرقم وبالتالي لا محل للقول بوقوع جريمة السرقة. بيد أن استعمال هذا الحساب في السحب من الرصيد يثير مشكلة انطباق الوصف القانوني الصحيح على هذه الواقعة : هل هو وصف السرقة أو هو وصف النصب؟

قد يبدو أن وصف السرقة يسري على هذه الواقعة باعتبار أن استعمال رقم الحساب يُعد بمثابة استعمال مفتاح مصطنع في فتح آلة من الآلات [1] . بيد أنه يُلاحظ أن الأمر ليس استعمالا لمفتاح مصطنع أو حتى لمفتاح غير مصطنع وأن استعمال رقم الحساب يترتب عليه تسليم ناقل للحيازة الكاملة اي أن الأمر لا يتعلق بالسرقة التي تفترض عدم التسليم . هذه السرقة لا تقع مع التسليم إلاّ في حالة ذلك التسليم الناقل لليد العارضة ، الأمر الذي لا يتوافر في هذا الفرض . كما يُلاحظ أن هذا التسليم يتم بناء على حيلة تتمثل في استعمال رقم الحساب الذي يخدع الآلة المنظمة لصرف الحساب من البنوك . هذه الحيلة يسري عليها وصف الاحتيال في جريمة النصب . ذلك أن مقتضى استعمال رقم الحساب أن يخدع الآلة ، موهما إياها بأن المتهم هو صاحب الحساب أو مفوض (وكيل) من قبل صاحب الحساب في صرف مبالغ مالية منه . ويُعد ذلك استعمالا لوسيلة من وسائل الاحتيال التي ينص عليها قانون العقوبات والتي تتمثل في استعمال صفة غير صحيحة . لذا نرى أن الوصف الصحيح لتلك الواقعة يتمثل في النصب وليس السرقة. وقد سبق القول بأنه لا يوجد في القانون ما يحول دون وقوع جريمة النصب على الآلة[2] .

ويُضاف إلى الوصف السابق وصف مرتبط ؛ وهو وصف التزوير في أوراق البنوك . ذلك أن المتهم ينتحل شخصية الغير ويتم تدوين ذلك الكذب في أوراق البنوك . هذا الكذب المتمثل في تغيير الحقيقة يتم تدوينه في أوراق الحساب ويتم إخطار صاحب الحساب به ؛ أنه في تاريخ معين قام

(١) د. محمود نجيب حسني ، شرح قانون العقوبات - القسم الخاص ، دار النهضة العربية ، ١٩٨٨ ص ٨٥٢؛ د. عبد العظيم مرسي وزير ، جرائم الأموال ، دار النهضة ١٩٨٣ ص ٨٥ .
(٢) انظر سابقا رقم ٤٦ .

بسحب جزء من الرصيد بنفسه ، أو بواسطة نائب عنه . ويلاحظ أن قانون الجزاء الكويتي قد أورد نصا خاصا في تزوير أوراق البنوك قرر فيه عقوبة الجناية لهذا النوع من التزوير . ذلك هو نص المادة ٢٥٩ من قانون الجزاء الذي يجري على أنه " إذا ارتكب التزوير في محرر رسمي أو في ورقة من أوراق البنوك كانت العقوبة الحبس مدة لا تجاوز سبع سنوات ... ".

١١٦- استعمال شبكة الإنترنت في التأثير على الأداء السليم للبورصة :

قد يعمد بعض المسئولين في الشركات إلى بث معلومات كاذبة عن أصول شركاتهم وحساب الأرباح والخسائر فيها . وقد ويؤدي ذلك إلى ارتفاع كبير في أسهم تلك الشركات في البورصة حيث يقبل الجمهور على شراء تلك الأسهم وهو واقع تحت هذا التغرير. فإذا ما اتضح الأمر انهارت تلك الأسعار إلى أدنى مستوياتها وتسبب ذلك في خسائر كبيرة . وقد حدث ذلك بالفعل في الولايات المتحدة الأمريكية[1].

وتدرك التشريعات خطورة التأثير على الأداء السليم لبورصة الأوراق المالية ، لذا فإنها تحرص على الحفاظ على ثقة الجمهور في سوق الأوراق المالية (البورصة) وتسن من التشريعات ما يكفل سلامة الأسواق المالية . ويقتضي ذلك كله أن تأتي البيانات المالية الخاصة بالشركات صحيحة ، غير متضمنة لما من شأنه أن يؤدي إلى التغرير بالمساهم أو مشتري السند . من هذه التشريعات القانون المصري رقم ٩٥ لسنة ١٩٩٢ بإصدار قانون سوق رأس المال . فتنص المادة ٦٣ من هذا القانون على أنه " مع عدم الإخلال بأية عقوبة أشد ، منصوص عليها في أي قانون آخر يُعاقب بالحبس لمدة لا

---

(١) انظر :
Jim Drinkhall, Computer Fraud , Internet Fraud , Journal of Financial Crime , January 1997 , p. 258 .

تزيد على خمس سنوات ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تزيد على مائة ألف جنيه ، أو بإحدى هاتين العقوبتين : ١ - ... ٢ - ... ٣ - كل من أثبت عمدا في نشرات الاكتتاب أو أوراق التأسيس أو الترخيص أو غير ذلك من التقارير أو الوثائق أو الإعلانات المتعلقة بالشركة بيانات غير صحيحة أو مخالفة لأحكام هذا القانون أو غيّر في هذه البيانات بعد اعتمادها من الهيئة أو عرضها عليها . ٤ - كل من أصدر عمدا بيانات غير صحيحة عن الأوراق المالية التي تتلقى الاكتتاب فيها جهة مرخص لها بتلقي الاكتتابات . ٥ - كل من زور في سجلات الشركة أو أثبت فيها عمدا وقائع غير صحيحة أو عرض تقارير على الجمعية العامة للشركة تتضمن بيانات كاذبة . ٦ - كل من عمل على قيد سعر غير حقيقي أو عملية صورية أو حاول بطريق التدليس التأثير على أسعار السوق . ٧ - كل من قيّد في البورصة أوراقا مالية بالمخالفة لأحكام هذا القانون ولائحته التنفيذية.

يبقى أن تدرك التشريعات المختلفة خطورة الاستعانة بشبكة الإنترنت كوسيلة لارتكاب الجرائم السابقة . لذا فإنه من المناسب أن تورد تلك التشريعات ظرفا مشددا للعقوبة في حالة وقوع الجريمة بطريق الإنترنت .

١١٧ - استعمال شبكة الإنترنت في ارتكاب جرائم السب والقذف :

قد تُستعمل شبكة الإنترنت كوسيلة لارتكاب جرائم السب والقذف . من ذلك أن يذيع المتهم ألفاظ السباب أو القذف من خلال موقع على الشبكة . هذا المواقع يتوافر فيها ركن العلانية . ولا يحول دون وقوع الجريمة أن ينشئ المتهم موقعا باسم شخص آخر بغرض حجم هويته الحقيقية . وقد يتم إيصال الألفاظ المجرّمة من خلال البريد الإلكتروني e - mail . وقد يُنشئ المتهم بريدا إلكترونيا باسم شخص وهمي ، بل إنه قد ينشئ هذا النوع

من البريد الذي يرسل منه ألفاظ السب أو القذف باسم شخص حقيقي ويرسل إلى شخص أو عدة أشخاص رسائل يعترف فيها بارتكاب جرائم أو أفعال ماسة بالكرامة أو بالسمعة باسم صاحب البريد . وبالتالي فإنه ينسب إليه صدور مثل هذه الإقرارات أو الاعترافات التي تسيء إليه.

١١٨- استعمال شبكة الإنترنت في ارتكاب جرائم الإرهاب والاتجار بالمخدرات :

قد يستعمل المجرمون شبكة الإنترنت في ارتكاب بعض الجرائم الخطيرة من جرائم المخدرات وجرائم الإرهاب ، مستغلين في ذلك سرعة وسهولة الاتصال على المستوى الدولي بين العصابات الإجرامية في تلقي التعليمات الإجرامية وتنفيذها والهروب من متابعة السلطات القضائية ومساعديها .

هذه الأسباب تدعو إلى التعاون بين السلطات عبر الدول المختلفة ، على المستوى الوقائي لمنع وتوقي ارتكاب هذه الأنواع الخطيرة من الجرائم، وكذلك على المستوى الجنائي ، وذلك بتشديد العقاب في حالة ارتكاب إحدى هذه الجرائم عن طريق شبكة الإنترنت. وسوف نشير إلى مشكلات الاختصاص القضائي المرتبطة بوقوع الجرائم بطريق الإنترنت.

١١٩- استعمال شبكة الإنترنت في الاعتداء على سرية المراسلات :

قد يتخذ البعض من شبكة الإنترنت وسيلة للاطلاع على المراسلات بين مستخدمي تلك الشبكة[1]. وهنا يلاحظ أن النص التقليدي الذي يحمي المراسلات لا يسري على المراسلات التي تتم بطريق الكمبيوتر. ذلك أن نص المادة ١٥٤ عقوبات صريح في سريانه على المكاتيب المسلمة إلى البوستة

---

(١) د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، رسالة ، طنطا ٢٠٠ ص ٢١٨ .

. فتنص المادة السابقة على أن "كل من أخفى من موظفي الحكومة أو البوستة أو مأموريهما أو فتح مكتوبا من المكاتيب المسلمة للبوستة أو سهل ذلك لغيره يعاقب بالحبس أو بغرامة لا تزيد على مائتي جنيه وبالعزل في الحالتين . وكذلك كل من أخفى من موظفي الحكومة أو مصلحة التلغرافات أو مأموريهما تلغرافا من التلغرافات المسلمة إلى المصلحة المذكورة أو أفشاه أو سهل ذلك لغيره يعاقب بالعقوبتين المذكورتين ".

وواضح أن النص السابق يقتصر في حمايته على المراسلات البريدية والتلغراف ، كما أن ينحسر في حمايته من ناحية أخرى وهي الفاعل في الجريمة. ذلك أن النص السابق لا يخاطب إلاّ موظفي الحكومة أو البوستة. وبالتالي فإن النص لا يسري على الأفراد العاديين الذين لم يشتركوا مع فاعل أصلي هو الموظف العام أو العاملين بالبوستة . كما أن النص لا يسري إلاّ على "المكاتيب " ، وهو الأمر الذي لا يسعفنا في خصوص المراسلات بطريق الكمبيوتر والإنترنت.

ومن ناحية أخرى فإن حكم المادة ٣٠٩ مكررا عقوبات يحمي الحياة الخاصة من استراق السمع على المحادثات التي تجري في مكان خاص أو بطريق التليفون . ذلك أن النص كما هو واضح لا يسري إلاّ على المحادثات التي تجري في مكان خاص أو بطريق التليفون .

وقد اتجه رأي إلى إعمال نص المادة ٣٠٩ مكررا من قانون العقوبات على المحادثات التي تجري عن طريق شبكة الإنترنت استنادا إلى أن تشغيل الإنترنت يتم بالاستعانة بالخط التليفوني [1] . غير أننا لا ننضم إلى هذا الرأي

---

(١) د. جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، دار النهضة العربية ، ٢٠٠١ ص ٢٥ .

ذلك أن الاتصال عن طريق شبكة الإنترنت يختلف عن الاتصال عن طريق التليفون . فشبكة الإنترنت هي شبكة عالمية عنكبوتية لا يتحقق لها سرية الاتصال التي قُصد إلى توفيرها بالنسبة للاتصالات الهاتفية. يُضاف إلى ذلك ما يمكن أن يعترض عليه البعض من أن محل الحماية في نص المادة ٣٠٩ مكررا عقوبات هو المحادثات الشفوية بين المتخاطبين ، بينما الاتصال عن طريق شبكة الإنترنت يتم بطريق مكتوب أي في شكل رسائل وليس في شكل محادثة من النوع المقصود في المادة السابقة . وما دام القياس في مواد التجريم أمر محظور ، فإن لا يمكن أن يمتد التجريم الوارد في المادة السابقة إلى الاتصال عن طريق شبكة الإنترنت.

ومن هنا نرى ضرورة التدخل بنص لحماية المراسلات التي تتم عن طريق الكمبيوتر، سواء كان ذلك بطريق شبكة الإنترنت أو بالشبكات الداخلية. ولا محل عندئذ لاقتصار النص في حمايته على موظفي الحكومة والعاملين بهيئة المواصلات السلكية أو اللاسلكية أو لاقتصارها على المحادثات الشفوية التي تجري في مكان خاص أو بطريق التليفون.

١٢٠- ضرورة حماية جمهور الناس من فوضى الدعاية التجارية:

ترتب على اشتراك العديد من الناس في شبكة الإنترنت أن استخدمت كثير من الشركات التجارية صندوق البريد الإلكتروني لهؤلاء المشتركين في إرسال عديد من العروض التجارية والإعلانات التجارية التي تسبب إزعاجا للجمهور وتضييعا لوقتهم وترتب مصروفات على عاتقهم ، فضلا عما يقع من خلال تلك الدعايات من جرائم للنصب على الجمهور . لذلك استشعر المشرع في الولايات المتحدة الأمريكية ضرورة حماية الجمهور من تلك الظاهرة وسن قانون , Netizens Protection Act ١٩٩٧ . وقد ألزم هذا

القانون أي شركة تجارية بعدم إرسال إعلانات وعروض تجارية إلاّ بشرط وجود علاقة سابقة مع صاحب الصندوق الإلكتروني تسمح بذلك . ويلتزم مرسل تلك الإعلانات أو العروض بذكر ما يفيد تحديد شخصيته وصندوق بريده الإلكتروني .

١٢٦- الاكتفاء باعتبار جرائم الإنترنت من جرائم الخطر:

من الضروري الاكتفاء باعتبار جرائم الإنترنت من جرائم الخطر وعدم اشتراط وقوع ضرر معين من جرّاء استعمال تلك الشبكة في ارتكاب جرائم معينة . ومؤدى ذلك أنه لا يشترط وقوع الجريمة التي ينوي المتهم ارتكابها من التداخل في بعض أجهزة الكمبيوتر كتلك التي تنتمي إلى الإدارات العامة أو المؤسسات المالية أو الشركات التي تقوم بنشاط في التجارة الدولية.

يترتب على ذلك أنه لا يلزم لوقوع الجريمة أن يتوصل المتهم إلى الاستيلاء على أموال الغير في جريمة سرقة أو نصب أو خيانة أمانة . كما لا يلزم وفقا لهذا الاتجاه أن يرتكب الفاعل جريمة من جرائم الإرهاب أو جرائم المخدرات ، بل يكفي أن تتجه نيته إلى ارتكاب إحدى هذه الجرائم عن طريق استعمال شبكة الإنترنت.

ويمكن تصور النشاط المؤثم في شكل إعطاء تعليمات أو إدخال برامج أو كلمات سر أو أرقام بطاقات خاصة لارتكاب جرائم معينة يحددها المشرع. من هذه الجرائم جرائم السرقة والنصب وخيانة الأمانة وجرائم الإرهاب وجرائم المخدرات.

المطلب الثاني

تحقق ركن العلانية من خلال شبكة الإنترنت

١٢٢- البث عن طريق شبكة الإنترنت :

تحقق شبكة الإنترنت ركن العلانية الذي يتطلب القانون توافره لوقوع بعض الجرائم مثل جريمة السب العلني وجريمة القذف وجريمة الفعل الفاضح العلني. وترجع العلانية إلى حقيقة أن الكتابة والصور التي تظهر على الكمبيوتر من خلال استعمال شبكة الإنترنت يُتاح لكل شخص الاطلاع عليها . ولما كانت جريمة السب والقذف قد تقع من خلال الكتابة التي تمس الشرف والاعتبار ، ولما كان ركن العلانية يتوافر بظهور هذه الكتابة أو الرسوم المؤثمة على شبكة الإنترنت ، فإن تلك الجرائم تتكامل لها أركانها القانونية.

وبالمثل فإن جريمة الفعل الفاضح العلني يتوافر لها العلانية ، وذلك عن طريق بث الصور والمناظر الفاضحة بطريق الإنترنت . والحقيقة أن الصعوبة القانونية التي تثور هنا لا تتمثل في ركن العلانية الذي لا يثير شكا، بقدر ما تتصل بالركن المادي في جريمة الفعل الفاضح . فمن القواعد المقررة أن هذا الركن المادي يتمثل في قيام الجاني بنشاط . هذا النشاط هو فعل معين[١]. ولما كان الأمر يتعلق بصور ومناظر وأفلام ، فإن ذلك قد يثير صعوبة قانونية نظرا لأن الجاني لا يقوم هنا بالفعل الفاضح وإنما ببث الصور والمناظر والأفلام [٢]. بيد أنه يمكن الرد على هذه الصعوبة القانونية بالقول بأن هناك فعلا منسوبا إلى الجاني يتمثل في بث هذه المواد الفاضحة . هذا البث يعتبر

---

(١) انظر عكس ذلك : د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، المرجع السابق ، ص ٢٣٥ .

(٢) د. ادوار غالي الدهبي ، الجرائم الجنسية ، ١٩٩٧ ص ٣٧٢ ؛ د. إبراهيم حامد طنطاوي ، جرائم العرض والحياء العام ، المكتبة القانونية ١٩٩٨ ص ٢٢١ .

فعلا فاضحا مادام محله هو تلك المواد الفاضحة.

١٢٣- إرسال الرسائل عن طريق البريد الإلكتروني :

قد تقع بعض الجرائم عن طريق إرسال رسائل بالبريد الإلكتروني e – mail . هذا النوع من الإرسال لا يتحقق به العلانية بحسب الأصل ، لأنه بمثابة إرسال رسالة إلى صندوق بريد شخص معين. ومن ثم فإذا كان القانون يتطلب ركن العلانية في جريمة معينة ، فإن هذه الجريمة لا تقع. من ذلك جريمة القذف، وجريمة السب العلني. أما إذا عمد المتهم إلى إرسال تلك الرسائل إلى عدد من الأشخاص بدون تمييز [١] ، فإن ركن العلانية – في رأينا – يتحقق. فهذا يسري عليه ما اعتبره القضاء المصري محققا لركن العلانية في خصوص من يقدم عددا من الشكاوى إلى جهات متعددة بدون تمييز[٢] . كما يعتبر محققا لركن العلانية أن يعمد المتهم إلى ترك الرسالة في مكان يمكن لغيره من مستخدمي الشبكة قراءتها.

على عكس ذلك فإن إرسال الرسائل إلى صندوق البريد الإلكتروني لشخص معين لا يتوافر فيه ركن العلانية . كما أن امتداد الحماية الجنائية المقررة للمراسلات الخاصة عن طريق البريد وفقا للنصوص التقليدية في قانون العقوبات إلى المراسلات بطريق البريد الإلكتروني ليست ثابتة ، نظرا لأن تلك الحماية كانت مقررة أصلا للمراسلات الورقية [٣]. ولما كانت هناك إمكانية لاعتراض تلك الرسالة الخاصة ، بطريق الإنترنت، بين لحظة إرسالها

---

(١) د. جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، دار النهضة العربية ، ٢٠٠١ ص ٧١ وص ٩٩؛ د. سعيد عبد اللطيف ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت ، دار النهضة العربية ١٩٩٩ ص ٢٢٧ .

(٢) نقض ١٧ يونيه سنة ١٩٤٦ ، مجموعة القواعد القانونية جـ ٧ رقم ١٩٩ ص ١٨٥ ؛ ٩ نوفمبر سنة ١٩٧١ أحكام النقض س ٢٢ رقم ١٦٣ ص ٦٦٩ .

(٣) انظر

Université de Poitiers , Faculté de Droit et de Sciences sociales, " Les nouvelles pratiques délictuelles liées aux technologies de la communication " , Actes du Juriscope 96, Publication du Magistère en Droit de la Communicatique, P.U.F., 1999,p. 92.

ولحظة استقبالها ، فإن ذلك يثير التساؤل حول اعتباره من قبيل فتح الرسالة الخاصة لقراءتها. بيد أنه نظرا لاختلاف اعتراض الرسالة عن فتح الرسالة ، فإن الأمر قد يثير صعوبة قانونية في تطبيق القواعد التقليدية على الوضع الخاص بالإنترنت ، الأمر الذي يقتضي تدخلا تشريعيا بنصوص خاصة لمقابلة هذا الوضع الخاص.

١٢٤- إرسال الرسالة عن طريق قائمة الرسائل:

قد يشترك مستعمل شبكة الإنترنت في قائمة تضم عدة أسماء من بلدان مختلفة يكون الغرض منها أن تظهر رسالة كل مشترك منهم في صندوق رسائله. وبناء عليه فإن المرسل لا يضّطر إلى إرسال عدة رسائل بنفس المضمون إلى كل شخص وتتعدد الرسائل بهذه الصورة . فليس عليه إذن إلاّ أن يرسل الرسالة مرة واحدة إلى قائمة المشتركين فتظهر بصورة تلقائية في صندوق البريد الآلي لكل شخص من هؤلاء الأشخاص ليقوم بالرد على تلك الرسالة أو يعلم بها .

وتثير هذه الطريقة تساؤلا حول توافر ركن العلانية . فإذا كان الأمر واضحا بالنسبة لإرسال رسالة إلى شخص واحد عن طريق بريده الإلكتروني (e – mail) فإن الأمر يختلف بالنسبة لقائمة المراسلة (mailing – list) ، ذلك أن الأشخاص المشتركين في هذه القائمة عددهم ليس صغيرا، كما أنه لا توجد علاقة شخصية تربط هؤلاء المشتركين . ومن هنا يمكن القول بتوافر ركن العلانية في حالة ارتكاب جريمة من الجرائم التي تقتضي توافر هذا الركن[1].

---

(١) انظر عكس ذلك : د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، المرجع السابق ، ص ٢٣٥ .

نتائج الدراسة

في نهاية دراستنا عن دور قانون العقوبات في مكافحة جرائم الكمبيوتر نخلص إلى نتائج ، أهمها:

١- على الرغم من أن التشريعات الحديثة أدرجت برامج الكمبيوتر ضمن المصنفات التي يحميها قانون حماية حق المؤلف ، فإن الحماية الجنائية التي يقدمها ذلك القانون يرد عليها من القيود ما يحد من فعاليتها بالنسبة لبرامج الكمبيوتر .

٢- لا يكفل قانون حماية حق المؤلف الحماية القانونية للمعلومات المبرمجة بالكمبيوتر ، ذلك أن هذا القانون يحمي المصنفات أي البرامج وليس المعلومات .

٣ - إن القواعد التقليدية في قانون العقوبات غير ملاءمة لمواجهة جرائم السرقة والنصب وخيانة الأمانة وإخفاء الأشياء المتحصلة من جريمة إذا وقعت تلك الجرائم على معلومات .

٤ - يرجع السبب في عدم الملاءمة سابقة الذكر إلى الطبيعة الخاصة للمعلومات إذا ما قورنت بغيرها من منقولات . ذلك أن المعلومات لها طابع معنوي .

٥ - إن القضاء الفرنسي اجتهد في تحديد مفهوم جديد للاختلاس يتمشى مع ما للمعلومات من طبيعة خاصة على ما سلف بيانه .

٦ - إن أحكام القضاء الفرنسي استقرت على أن المعلومات لا تكتسب صفة المال المنقول الذي تحميه جرائم الأموال إلاّ إذا كانت مدوّنة على دعامة مادية .

٧ - لا شيء يحول دون اعتبار المعلومات المبرمجة من قبيل المنقولات وبالتالي إعمال قواعد السرقة والنصب وخيانة الأمانة عند قيام المتهم بنسخها على نحو ما سبق أن أوضحناه .

٨ - إن الاختلاس كنشاط في جريمة السرقة أصبح فكرة مقبولة لدى القضاء الفرنسي عند قيام المتهم بنسخ لمعلومات المبرمجة ، وذلك بشرط أن يتصل الفاعل بالدعامة المادية في الوقت اللازم للنسخ .

٩ - لا شيء في القانون يحول دون وقوع النصب على الكمبيوتر ، كما لو كان هذا الجهاز ينتمي إلى بنك مثلا .

١٠ - إن انطباق وصف تزوير المحررات على تغيير البيانات الواردة في النظام (الكمبيوتر) لم ينل إجماعا في الرأي . ومن المناسب التدخل التشريعي في تحديد مفهوم التزوير بحيث يشمل تغيير الحقيقة في بيان مكتوب أو في معلومات مبرمجة ، على غرار ما فعلته تشريعات عديدة .

١١ - لو انتهينا إلى انسحاب وصف التزوير على تغيير الحقيقة في المعلومات المدونة على دعامة مادية ، فإن ذلك لا يكفي لتوفير حماية جنائية كافية لتلك المعلومات ، ذلك أن من تلك المعلومات ما لم يعد للاحتجاج به في إثبات حق أو مصلحة قانونية على ما سلف بيانه .

١٢ - من الأسباب التي تحول دون توافر صفة المحرر للبيانات التي لا تزال مسجلة في الكمبيوتر عدم توافر نية استعمال المحرر فيما زُور من أجله . لذا كان من حسن السياسة الجنائية إيراد نصوص خاصة تعاقب على التغيير في تلك البيانات .

١٣ - حسنا فعلت التشريعات المقارنة عندما أفردت نصوصا خاصة للعقاب على تغيير البيانات المبرمجة ، حتى تتغلب على الصعوبة القانونية المتمثلة في اعتبار تلك البيانات من المحررات قبل طبعها في أوراق .

١٤ - استشعرت التشريعات الحديثة خطورة الكمبيوتر على الحريات الشخصية ووضعت من القواعد ما يكفل عدم إساءة استعمال ذلك الجهاز في الاعتداء على تلك الحريات .

١٥ – إن الحماية الوقائية للأفراد من إساءة استعمال الكمبيوتر لا تقتصر على المعلومات السرية المتعلقة بالحياة الخاصة فقط ، ولكن تمتد لتشمل سائر البيانات الشخصية مثل العمل والتعليم والزواج والانتماء إلى حزب أو نقابة معينة وممارسة نشاط سياسي معين ، إلى غير ذلك من البيانات الشخصية .

١٦ – إنه من المناسب إيراد نصوص خاصة لتجريم التداخل في نظام الكمبيوتر وتغيير البيانات الواردة فيه والتحايل للاستفادة بخدمات (وقت الكمبيوتر) أو برامج يقدمها نظام الكمبيوتر، وكذلك إتلاف البيانات المبرمجة فيه . وقد تدخل المشرع في قوانين أوربية وأمريكية بالتجريم في هذا المجال. ويرجع ذلك إلى الصعوبة القانونية التي لا تزال قائمة لدى البعض حول تطبيق القواعد التقليدية في جرائم الأموال (السرقة والنصب وخيانة الأمانة) في مجال المعلومات المبرمجة.

١٧ – من اللازم حماية المعلومات المبرمجة من التجسس عليها والاطلاع عليها بأي شكل من الأشكال .

١٨ – من الواجب حماية المراسلات التي تتم بطريق الكمبيوتر نظرا لعدم انطباق نصوص حرمة المراسلات البريدية عليها .

١٩ – بالإضافة إلى تطبيق القواعد التي تحكم سرية المراسلات ، فإنه يتعين تجريم اعتراض الرسائل المتبادلة بين أجهزة الكمبيوتر، بوصفه مشكلا لجريمة التداخل في النظام وليس فقط مخالفا لسرية المراسلات . ويمكن الوصول إلى هذه الغاية عن طريق تجريم التداخل مع بيان أن هذا التداخل يشمل اعتراض المعلومات المرسلة بين أكثر من جهاز .

٢٠ – من المفيد إيراد نصوص خاصة لتجريم سرقة خدمة الكمبيوتر " وقت الكمبيوتر " دون رضاء صاحب الحق فيه .

٢١ - يلزم سن نصوص خاصة لحماية البرامج المشفرة من محاولة الحصول عليها بدون وجه حق ، إضرار بالشركات المرسلة لها ، وذلك باستعمال أدوات مقلدة لاستقبال ذلك الإرسال أو لتحسين صورته .

٢٢ - من الضروري أن نأخذ في اعتبارنا الوضع الخاص لاستخدام شبكة الإنترنت في ارتكاب الجرائم ، سواء أكانت جرائم أموال أم جرائم الإرهاب أو الاتجار في المخدرات أم الاستغلال الجنسي للأطفال أو غيرها من الجرائم التي لها تقع في أكثر من دولة .

٢٣ - من الضروري زيادة التعاون الدولي في مجال الجرائم التي تتم عبر الدول بطريق الكمبيوتر والإنترنت . ويصبح من الضروري عقد الاتفاقيات الدولية للتعاون القضائي في مرحلة التحقيقات والمحاكمة والاعتراف بالأحكام الأجنبية وكذلك لتسهيل تسليم المجرمين في هذا المجال .

٢٤ - العبرة في تحديد اختصاص الدولة بالمحاكمة هي بأركان الجريمة وليس بالأثر ، وبالتالي فإن مشاهدة جريمة على الإنترنت في جميع العالم لا يعطي الاختصاص لكل دولة من دول العالم بمحاكمة المتهم .

٢٥ - من المهم بمكان تنظيم المسئولية الجنائية لمقدم الخدمات provider على شبكة الإنترنت .

٢٦ - من الضروري تقرير المسئولية الجنائية للشخص المعنوي عن جرائم الكمبيوتر والإنترنت التي تصدر عن الأجهزة التابعة لهذا الشخص أو لحسابه. ذلك أن الفاعل قد لا يُعرف في حالات كثيرة . وتتم تقرير تلك المسئولية بوصف العمد. ولكن ليس هناك ما يحول دون أن تقوم بالوصف غير العمد في بعض الحالات يحددها المشرع . وبديهي أن الجزاء الجنائي ينحصر في الجزاءات غير الماسة بالحرية مثل الغرامة وقفل المنشأة وسحب التراخيص .

الباب الثاني

ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات

موضوع الدراسة :

تتميز إجراءات الدعوى الجنائية في بعض مظاهرها بطابع خاص في مجال جرائم تقنية المعلومات كثيرا ما يضفي عليها طابعا من الذاتية إذا ما قورنت بإجراءات الدعوى الجنائية في غيرها من الجرائم. ويرجع ذلك إلى عدة أسباب منها ما يلي:

- توافر البيانات المبرمجة في أجهزة جهات عامة وخاصة متعددة،
- ارتباط كثير من أجهزة الكمبيوتر بعضها ببعض في شبكة واحدة،
- ما تتميز به شبكة الانترنت من طابع يجعلها متاحة للجميع كما أنها متوغلة في أماكن عديدة بل وفي دول العالم المختلفة.

وتنعكس هذه الذاتية على مظاهر شتى في أثناء سير الإجراءات الجنائية بدءا من مرحلة جمع الاستدلالات وانتهاء بالمحاكمة ومرورا بمرحلة التحقيق الابتدائي. وسوف نعرض لما تتميز به إجراءات جمع الاستدلال وإجراءات التحقيق الابتدائي ومرحلة المحاكمة من خصائص لها ذاتية تتميز بها عن الإجراءات الجنائية في الجرائم الأخرى. هذه الجوانب التي تنفرد بها تلك إجراءات الدعوى في مجال هذا النوع من الجرائم هي موضوع الدراسة في هذا البحث.

أهمية الدراسة:

ترجع أهمية البحث إلى تنامي دور التعاملات الإلكترونية، الأمر الذي طرح تحديات عديدة أمام رجل القانون في مجال مكافحة جرائم تقنية المعلومات (الكمبيوتر والإنترنت)، يتعين البحث عن إجابة لها فيما يلي من سطور.

كما ترجع أهمية البحث إلى صدور القانون رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، وهو ما يستدعي الدراسة لبيان ما تضمنه من مزايا وما يعتوره من أوجه للقصور.

إشكالية الدراسة:

يستهدف البحث الإجابة إلى بعض الأسئلة والتساؤلات، من أهمها؛ ما هي أوجه الذاتية التي تميز الإجراءات الجنائية في مرحلة جمع الاستدلالات في مجال الجرائم الإلكترونية ؟ ما هي أوجه الذاتية في مرحلة التحقيق الابتدائي؟ وما هي تلك الأوجه في مرحلة المحاكمة؟

خطة الدراسة:

سوف نقسم تلك الدراسة إلى ثلاثة مباحث:

المبحث الأول ويعالج ذاتية إجراءات جمع الاستدلالات في مجال جرائم تقنية المعلومات،

ويعالج المبحث الثاني ذاتية إجراءات التحقيق في مجال جرائم تقنية المعلومات،

بينما يتناول المبحث الثالث ذاتية إجراءات المحاكمة في مجال جرائم تقنية المعلومات

الفصل الأول

ذاتية إجراءات جمع الاستدلالات

في مجال جرائم تقنية المعلومات

- الطابع الخاص لتحريات رجال الضبط على شبكة الإنترنت:

لرجل الضبط القضائي أن يدخل الأماكن العامة على شبكة الإنترنت التي للشخص العادي أن يدخلها كالمواقع المختلفة ولو كان الدخول إليها معلقا على دفع مقابل مالي، وتصح الإجراءات ويجوز الاستناد إليها كدليل في الدعوى. تطبيقا لذلك قُضي في فرنسا بأن لرجل الضبط القضائي أن يتصل بشبكة "الميناتل" وأن يقرأ ما عليها من رسائل دون تعديل في تجهيزها شأنه في ذلك شأن الشخص العادي(١).

بيد أنه ليس لرجل الضبط أن يستعين ببرامج اختراق للدخول إلى المواضع الخاصة مثل الايه ميل والماسنجر.

- أهم الخصائص العامة لتي تميز جمع الاستدلالات في مجال جرائم تقنية المعلومات:

تنفرد إجراءات جمع الاستدلالات في هذا النوع من الجرائم بخصائص تميزها عن إجراءات الدعوى في الجرائم التقليدية، من ذلك ما يلي:

١- مصدر التحريات في الجرائم التقليدية يعتمد بصفة أساسية على شهود الواقعة بينما لا تشكل شهادة الشهود الوسيلة الأساسية لجمع التحريات في جرائم الكمبيوتر. فالشاهد في جرائم الكمبيوتر والانترنت هو

(1) Crim.25 oct.2000, Bull. Crim. n ° 317; Dr. penal2001.Comm.27, obs. Maron.

شخص متخصص من الفنيين في هذا المجال يعتمد عليه رجل الضبط، وقد يكون رجل الضبط متخصصا فيقوم بهذا الدور المباشر في تجميع التحريات عن هذا النوع من الجرائم ، وهذا يبرز أهمية هذا الدور.

٢- ضرورة الإعداد الخاص للقائمين على جمع الاستدلالات والتحقيق في جرائم تقنية، ذلك أن رجال الضبط القضائي غير المدربين على الكمبيوتر ليس بمقدورهم جمع التحريات عن هذا النوع من الجرائم. ويؤكد ذلك على وجوب إنشاء وحدات متخصصة من رجال الشرطة والمتعاونين معهم في هذا المجال لمكافحة هذا النوع من الجرائم.

- جواز الاستعانة بالمعلومات التي هي في حوزة أجهزة الدولة والأجهزة الخاصة لجمع التحريات عن الجريمة؛

فالقاعدة أن رجل الضبط القضائي من سلطتهم، بل من واجبهم أن يجمعوا المعلومات عن الجريمة ومرتكبيها وفقا للمادة (٢٤) من قانون الإجراءات والتي تنص على أنه "يجب على مأموري الضبط القضائي أن .... ويجب عليهم وعلى مرءوسيهم أن يحصلوا على جميع الإيضاحات ويجروا المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلمون بها بأي كيفية كانت وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة...". وفي نفس المعنى وبنفس التعبيرات نصت المادة (٣٥) من قانون الإجراءات الجنائية الإماراتي. والقاعدة تقضي بأن تجميع تلك البيانات عن الجرائم والمتهمين بها والمشتبهين بارتكابهم لها لا يخالف الحق في الحياة الخاصة، وبالتالي لا يخالف الدستور ولا يتسم بالبطلان، ما لم ينص القانون على عدم جواز ذلك.

وتطبيقا للقاعدة في صحة إجراءات جمع الاستدلالات، قُضي في كندا بصحة إجراءات التحريات التي قام بها رجال الضبط القضائي فيما استعانوا به من بيانات إدارة الكهرباء عن استهلاك صاحب أحد المنازل لكميات كبيرة من الكهرباء للتدليل على قيامه بزراعة مخدرات في حديقة منزله[1].

بيد أنه إذا حظر القانون الاستعانة بالمعلومات المتواجدة في أجهزة إدارة من الإدارات، فإنه لا يجوز للمحقق أو لمأمور الضبط القضائي أن يخالف هذا الحظر وإلاّ كان الدليل باطلا، ويحدث ذلك بالنسبة لبعض الإدارات مثل إدارات المستشفيات فيما تمتلكه من أجهزة تتضمن بيانات عن المرضى وإدارة الضرائب فيما تحتويه أجهزتها من معلومات عن الممولين. هذه الإدارات تلتزم بسر المهنة الذي يحول دون تعاونها مع رجال الضبط القضائي. ويستند ذلك إلى نص المادة (٣١٠) عقوبات مصري (المقابلة للمادة ٣٧٩ عقوبات اتحادي إماراتي) التي تعاقب على مخالفة سر المهنة.

٣- فرض واجب التعاون مع رجال الضبط القضائي على مزودي الخدمات:

هناك طائفتان من مزودي الخدمات؛ الطائفة الأولى وتضم من يقوم بتقديم خدمة إرسال أو استقبال الاتصالات السلكية والإلكترونية، والطائفة الثانية وتضم من يقدم للجمهور خدمة تتمثل في معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونية[2].

والحقيقة أن تلك الطائفة المهنية الجديدة في ظهورها لا تنتمي إلى طائفة الملتزمين بالسر المهني وفقا للمادة (٣١٠) من قانون العقوبات والتي تنص

---

(1) (Robert Scott Plant C. Sa Majesté la Reine (novembre 1993): http:/lexum.umontreal.ca/csc-scc/fr/pub/1993vol3html;David G. Masse, La prevue et l'utilisationdu courriel à l'insu de son auteur, www.masse.org/preuve-courriel.htm (2004) ،(R.C.S.284

(٢) د. شيماء عبد الغني محمد عطاالله، الحماية الجنائية للتعاملات الإلكترونية، دار النهضة العربية ، ٢٠٠٥ ص ٢١٠

على "كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم مودعا إليه بمقتضى صناعته أو وظيفته سر خصوصي أؤتمن عليه فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك يعاقب بالحبس مدة لا تزيد على ستة شهور أو بغرامة لا تتجاوز خمسمائة جنيه، ولا تسري أحكام هذه المادة إلاّ في الأحوال التي لم يرخص فيها قانونا بإفشاء أمور معينة كالمقرر في المواد ٢٠٢ ، ٢٠٣، ٢٠٤، ٢٠٥ من قانون المرافعات في المواد المدنية والتجارية". ويرجع السبب في رأينا إلى عدم التزامهم بسر المهنة إلى أنهم ليسوا من الأمناء الضروريين الذين يأتمنهم الناس على أسرارهم فيفضون إليهم بتلك الأسرار، بل إنهم قد يصادفون معلومات تتعلق بالغير بسبب إدارة أعمالهم المتمثلة في الإشراف على الاتصالات السلكية أو اللاسلكية أو الإلكترونية، أو بسبب قيامهم بصيانة الخطوط أو بالتدقيق على حسن سير تلك الخطوط.

ومن الواضح أن مزودي الخدمات سواء تعلق في مجال الخدمات السلكية أو اللاسلكية أو الإلكترونية يمكنهم أن يطلعوا على أسرار هامة للعملاء ، من هذه الأسرار:

- من يتصل بمن ، أي أطراف المراسلات الإلكترونية سواء عن طريق الإيه ميل أو عن طريق المحادثة المكتوبة أو الشفوية أو عن طريق المحادثة الصوتية.

- تاريخ حدوث اتصال معين بين جهازين من أجهزة المتصلين.

- المواقع التي يدخل عليها العملاء، يمكن لمزودي الخدمات أن يطلعوا على تلك المواقع التي يرجع إليها العملاء ومستخدمي شبكة الانترنت ، ويفيد ذلك أحيانا في تحديد مثلا طبيعة المواد التي يقرأها مستخدم الشبكة وبالتالي تحديد اتجاهه الإجرامي أحيانا، كما لو كان يرجع إلى مواقع تشرح تصنيع الديناميت وهو من المتهمين في جرائم الإرهاب.

وقد ظهر اتجاه في التشريعات المقارنة نحو السماح لمأموري الضبط

القضائي بالاطلاع على الأنواع السابقة من البيانات، مع إلزام مزودي خدمات الاتصالات السلكية والإلكترونية بالتعاون معهم. من تلك التشريعات قانون الإجراءات الفرنسي الذي ينص في مادته (٦٠-١) المعدلة بالقانون رقم ٢٠٤/ ٢٠٠٤ الصادر في ٩ مارس سنة ٢٠٠٤ على أنه "لمأمور الضبط القضائي أن يطلب من كل شخص، من كل مؤسسة من كل جهة خاصة أو عامة أو كل إدارة عامة، لديه مستندات تتعلق بالتحريات الجارية، ويدخل فيها تلك الصادرة عن أنظمة معالجة الكمبيوتر أو أنظمة معالجة المعلومات الاسمية، أن يسلمه هذه المستندات دون أن يكون لهؤلاء أن يتمسكوا – بدون وجه حق – بالالتزام بسر المهنة. وعندما يتعلق هذا الطلب بالأشخاص المشار إليهم في المواد ٥٦- ١ وما يليها حتى المادة ٥٦-٣، فإن تسليم هذه المستندات لا يمكن أن يتم إلاّ بموافقة منهم.

وباستثناء الطوائف المشار إليها في المواد ٥٦- ١ وحتى ٥٦-٣ ، فإن الامتناع عن إجابة الطلب السابق دون تأخير معاقب عليه بغرامة قدرها ٣٧٥٠ يورو. وتُسأل الأشخاص المعنوية جنائيا بنفس الشروط المنصوص عليها في المادة ١٢١- ٢ من قانون العقوبات الفرنسي عن الجريمة المنصوص عليها في هذه المادة"[1].

وتنتمي الاتفاقية الأوربية في شأن جرائم السيبر لسنة٢٠٠١ إلى هذا الاتجاه بنصها على أنه يجوز للدول الأطراف في هذه الاتفاقية أن تسمح

---

(1) " L'officier de police judiciaire peut requérir de toute personne, de tout établissementou organisme privé ou public ou de toute administration publique qui sont susceptible de détenir des documents intéressant l'enquête , y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les requisitions concernent des personnes mentionnées aux articles 56-1 à 56- 3, la remise des documents ne peut intervener qu'avec leur accord.
A l'exception des personnes mentionnées aux articles 56-1 à 3-56, le fait de d'abstenir de répondre dans les meilleurs délais à cette requisitions est puni d'une amende de 750 3 E. Les personnes morales sont responsables pénalement dans les conditions prévuées par l'article 2-12 1 du code pénal, du délit prévu par le présent alinéna."

لسلطاتها بالتحري عن البيانات المتعلقة بالمشترك (مادة ١٧). أما عن نوع تلك البيانات فقد عنيت الاتفاقية بالقول بأنها تشمل نوع خدمة الاتصال التي اشترك لفيها الشخص والوسائل الفنية لتحقيقها ومدة الخدمة وشخصية المشترك ورقم دخوله للحصول على تلك الخدمة والفواتير التي تُرسل إليه وأي معلومات تتعلق بطريقة الدفع أو أي معلومات أخرى تتعلق بأداء الخدمة أو بالاتفاق بين هذا المشترك وبين مزود الخدمة :

"b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement،

c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement"

ومؤدى ذلك أن لمأموري الضبط القضائي القيام بذلك من خلال سلطتهم في جمع الاستدلالات وبالتالي فإن الأمر لا يحتاج إلى سبق صدور إذن قضائي بذلك.

غير أن نصوص الاتفاقية لا تسمح بسلطة مأموري الضبط القضائي بالاطلاع على المراسلات في محتواها، فالأمر يحتاج عندئذ إذن قضائي ولا ينتمي إلى مجال التحريات في هذه الحالة وفقا لأحكام الاتفاقية.

ويعتبر ما سبق تطبيقا للقواعد العامة التي تحكم الاطلاع على بيانات الاتصالات الهاتفية والبيجر. فالتحريات التي يقوم بها رجال الضبط القضائي لمعرفة الأرقام التي اتصلت بالمجني عليه مثلا قبيل وقوع الجريمة (وعدد الاتصال ويوم وساعة الاتصال ومدة الاتصال وأصحاب تلك الأرقام) – أو

الأرقام التي اتصلت بالمتهم وهو مثلا من تجار المخدرات قبيل عقد الصفقة - تصح الاستناد إليها كقرينة للكشف عن الحقيقة ضد متهم معين. ونفس الأمر يقال عن الأرقام التي اتصلت بأجهزة البيجر وعدد الاتصال ويوم الاتصال وساعته.

تطبيقا لما سبق قُضي في الولايات المتحدة الأمريكية بأن وضع جهاز (pen register) لتسجيل أسماء طرفي الاتصال في صدد المحادثات الإلكترونية يجوز لرجل الضبط القضائي أن يقوم به دون شرط سبق الحصول على إذن قضائي بذلك، باعتباره منتميا إلى مجال جمع الاستدلالات وليس فيه إخلال بحرمة الحياة الخاصة[1].

- مدى حق ماموري الضبط القضائي في الاطلاع على محتوى الرسائل:

يمتنع على مزودي الخدمات السلكية أن يستمعوا إلى محتوى المحادثة بين طرفي الاتصال، لأن ذلك يُعد من قبيل التنصت على تلك المحادثات السلكية، وهو الأمر الذي يحظره القانون إلاّ بناء على أمر بذلك من السلطة المختصة. وتضع التشريعات المختلفة ضمانات للتنصت على المحادثات السلكية منها قانون الإجراءات المصري في مادته (٩٥) والتي تنص على أنه "لقاضي التحقيق أن .... يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراءات تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو مدد أخرى مماثلة".

---

(١) Smith v. Maryland ٤٤ ٧٣٥U.S.)١٩٧٩).

ومع ذلك فإن الأمر يختلف بالنسبة لمزودي خدمة الاتصالات الإلكترونية عن طريق أجهزة الكمبيوتر والإنترنت. هذه المحادثات تتم بطريق مكتوب من خلال الإيه ميل وعن طريق خدمة المحادثة الفورية "الماسنجر". هذه المراسلات في كلتا الصورتين يتم تخزين محتواها آليا في أجهزة مزود الخدمات، الأمر الذي يميز بينها وبين مزودي خدمات الاتصالات السلكية المحظور عليهم هذا التخزين.

وقد استدعى هذا الأمر أن يتدخل المشرع في تشريعات عديدة بوضع تنظيم يحدد مدة هذا التخزين، ومدى حق مزودي الخدمات في الاطلاع على محتوى تلك الرسائل، بالإضافة إلى - وهذا أمر هام - إلى حدود تعاونهم مع رجال الضبط القضائي في سبيل اطلاع هؤلاء الأخيرين على محتوى تلك الرسائل المخزنة أو في سبيل تمكينهم من الاطلاع على تلك المراسلات عند القيام بها. من تلك التشريعات القانون الفرنسي (la sécurité intérieure) في سنة ٢٠٠٣ الذي يلزم مزودي الخدمات بالكشف عن المعلومات التي لديهم لمأموري الضبط القضائي ، فلم يعد التزامهم قاصرا على أسماء المشتركين والأرقام التي يتصلون بها، بل امتد ليشمل محتوى الاتصالات الإلكترونية، الأمر الذي يبرز أن هذه الاتصالات الإلكترونية لا تتمتع بالحماية التي تتمتع بها الاتصالات السلكية (الهاتفية). وبالتالي فإن القانون الفرنسي أصبح يتمشي مع القانون الأمريكي المسمى بقانون حماية الحياة الخاصة في مجال الاتصالات الإلكترونية والقانون الوطني في مجال مكافحة الإرهاب Patriot Act . هذه القوانين تقيم هذا الالتزام على عاتق مزودي الخدمات فتضعف بالتالي من الحماية القانونية للاتصالات الإلكترونية منذ الاعتداء على مركز التجارة العالمية في نيويورك .

ويسبب ما تقدم تلزم التشريعات المختلفة مزودي الخدمات بالمحافظة على ما لديهم من بيانات سواء تتعلق بمستخدمي الشبكة أو محتوى الرسائل المتبادلة مدة معينة لتمكين السلطات العامة من الرجوع إليها. من تلك التشريعات قانون الأمن الداخلي الفرنسي والذي يلزم بمدة سنة قبل تخلصهم من تلك البيانات[١]. فتنص المادة ٦٠-٢ من قانون الإجراءات الفرنسي (المعدلة بالقانون رقم ٢٣٩ لسنة ٢٠٠٣ المعدلة بالقانون رقم ٢٠٤ لسنة ٢٠٠٤ على أن العاملين بالجهات العامة والخاصة التي تعمل من خلال أنظمة الكمبيوتر - وبناء على طلب من مأموري الضبط القضائي- عليهم أن يقدموا ما لديهم من معلومات، مع استثناء من منهم يكون ملتزما بالمحافظة على سر المهنة، مادامت تلك المعلومات لازمة للكشف عن الجريمة[٢].

وقد قننت المادة (٦٠-٢) إجراءات فرنسي التزام مزودي الخدمات (مثله في ذلك مثل أي جهة عامة أو خاصة) بالمحافظة على ما لديهم من معلومات تفيد في كشف الحقيقة وذلك لمدة لا تزيد على سنة واحدة وذلك بناء على طلب مأمور للضبط القضائي في مجال عمل التحريات اللازمة عن جريمة معينة ، ولكن بشرط سبق الحصول على إذن بذلك من قاضي الحريات والحبس بناء على طلب من النيابة العامة[٣].

---

(١) د. شيماء محمد عطاالله، المرجع السابق ص ٢٥٠.

(2) Sur demande de l'officier de police judiciaire, les organisms publics ou les personnes morales de droit privé, à l'exception de ceux visées au deuxième alinéa, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitement de données nominatives qu'ils administrent."...

(3) L'officier de police judiciaire, intervenant sur requisition du procureur de la Republique préalablement autorisé par ordonnance du juge des libertés et del la detention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés , sans délai, toutes measures propres à assurer la préservation , pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs"

يبين من النص السابق أن الأمر يتعلق بمحتوى الرسالة نفسها وليس بمجرد معلومات عن مرسل ومستقبل وزمان ومدة المراسلة. لذا فإن المشرع الفرنسي قد قيدها بوجوب الحصول على إذن من قاضي الحريات والحبس بناء على طلب من النيابة العامة لتخويل مأموري الضبط القضائي سلطة أن يأمر مزودي الخدمات بالمحافظة على محتوى تلك الرسائل تمهيدا لضبها لديهم والاطلاع عليها وتقديمها كدليل مشروع لإثبات الجريمة. وقد عاقبت المادة ٦٠-٢ إجراءات فرنسي على عدم الاستجابة للطلب السابق الذي استوفيت إجراءاته بعقوبة الغرامة التي لا تزيد على ٣٧٥٠ يورو[١].

وعلى الرغم من طبيعة عمل مزودي الخدمات على هذا النحو، فإنهم لا يلتزمون بالسر المهني[٢]. لذلك تتجه التشريعات المقارنة إلى إلزامهم بالتعاون مع مأموري الضبط القضائي، بحيث يفصحون عما يعلموه من تلك المعلومات والتي تفيد في كشف الحقيقة في أثناء القيام بالتحريات اللازمة نحو تلك الغاية.

وبناء عليه، فإنهم إن قاموا بإفشاء تلك المعلومات إلى رجال الضبط، فإن تلك المعلومات يصح الاستناد إليها كدليل أمام المحكمة فلا يشوبها البطلان. كما أن مزودي الخدمات لا يتعرضون للمساءلة الجنائية لقيامهم بذلك الإفشاء.

ويلاحظ أن ثمة فارقا بين إلزام مزودي الخدمات بتقديم ما لديهم من معلومات يتعلق بعضها بمحتوى الرسائل المتبادلة بين مستعملي الاتصالات

---

(1) Les organisms ou personnes visés au présent article mettent à la disposition les informations réquises par voie télématique ou informatique dans les meilleurs délais. Le fait de refuser de répondre sans motif légitime à ces requisitions est puni d'une amende de 3750 euros. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 2-121du code pénal de l'infraction prévue au present alinéa. La peine encourue par les personnes morales est l'amende, suivant les modalités prévues par l'article 38-131 du code penal.'

(٢) د. شيماء عبد الغني عطا الله ، المرجع السابق ص ٢١٢

الإلكترونية وبين التنصت على تلك المراسلات وقت وقوعها on line. فإذا كانت بعض التشريعات الأوربية والأمريكية قد بدأت تجيز إلزام مزودي الخدمات بتقديم ما لديهم من معلومات تتعلق بمحتوى الرسائل – وهذا أمر خطير لا تمشي مع حرمة الحياة الخاصة في المحادثات الكتابية الإلكترونية – ، فإن التنصت على تلك المحادثات حال وقوعها لم تسمح به التشريعات المختلفة إلاّ بناء على إذن قضائي. ويرجع ذلك إلى التماثل بين المحادثات الكتابية الإلكترونية والمحادثات الهاتفية ذات الطابع الشفوي. كما أنه قد ظهرت محادثات شفوية إلكترونية عن طريق استخدام شبكة الإنترنت لإتمام الاتصالات الهاتفية، لذا كان من الضروري إقامة التقارب بين المحادثات الإلكترونية والمحادثات الهاتفية.

ومما يضعف من الطابع الخاص للاتصالات الإلكترونية أنه يدخل في اختصاص مزودي الخدمات أن يدافعوا عن الاعتداء عليهم في شكل الاستيلاء على الخطوط أو الخدمات التي يؤدونها بمقابل للجمهور. عندئذ لهم أن يراقبوا هؤلاء المعتدين. ومن صور الاعتداء على شبكاتهم ما يقوم به البعض من زرع فيروسات من شأنها أن تخل بحسن سير النظام.

كما أن لهم أن يقوموا بمتابعة سير العمل اليومي لخدماتهم السلكية أو الإلكترونية، الأمر الذي يقتضى التنصت أحيانا على بعض المحادثات السلكية أو الإلكترونية لهذا الغرض. فإذا ما اكتشفوا أن هناك جريمة تقع أو أن هناك مخططا لوقوع تلك الجريمة، فإن لهم أن يقوموا بتبليغ رجال الضبط القضائي، كما أن شهادتهم تُقبل كدليل أمام القضاء، وقد انتهت المحاكم الأمريكية إلى ذلك في العديد من أحكامها[1]

وقد تضمن قانون حماية الحياة الخاصة في مجال الاتصالات

---

(1) Re Doubleclick Inc. Privacy Litigation Civ. ٠٦٤١, ١٥٤F. Supp.٢d ٤٩٦(S.D.N.Y, March ٢٨, ٢٠٠١); Re Pharmatrak, Inc. Privacy Lititgation , Civ. Act. No –١١٦٧٢–٠٠

الإلكترونية في الولايات المتحدة الأمريكية(E.C.P.A: Electronic Communication Privacy Act) نصا يجيز لمزودي الخدمات في مجال الاتصالات الإلكترونية أن يقوموا بإبلاغ مأموري الضبط القضائي عن معلومات تتعلق بارتكاب جريمة أو في حالة الاستعجال إذا كان هناك خطر الموت أو إيذاء جسمي يهدد الأشخاص وكذلك في حالة الجرائم التي تقع إخلالا بقانون حماية الطفل والذي تضمن أحكاما لتجريم الأفعال الجنسية الشاذة.

الفصل الثاني

ذاتية إجراءات التحقيق

في مجال جرائم تقنية المعلومات

بالإضافة إلى ما تتسم به إجراءات جمع الاستدلالات في مجال جرائم تقنية المعلومات من جوانب خاصة تميزها عن إجراءات الاستدلال في غيرها من جرائم، فإن إجراءات التحقيق الابتدائي تنطوي أيضا على جوانب خاصة لصيقة بما لهذا النوع من الجرائم من سمات خاصة، سوف نعرض لها في هذا الفصل.

- مدى وجوب صدور إذن قضائي لاعتراض أو تسجيل المحادثات الإلكترونية:

تظهر ذاتية المحادثات الإلكترونية من أن القانون لم ينص على تجريم اعتراضها وذلك على خلاف ما هو مقرر بالنسبة المحادثات الهاتفية. فتنص المادة ٣٠٩ مكررا عقوبات على تجريم استراق السمع على المحادثات الهاتفية بقولها "يعاقب بالحبس مدة لا تقل عن سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه: (أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طرق التليفون. (ب) التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص. ".

ونظرة إلى قانون العقوبات الاتحادي نجد أنه تضمن نصا بخصوص الاتصالات الهاتفية، عندما عاقب على استراق السمع على تلك المحادثات بقوله في المادة (٣٨٠) عقوبات اتحادي "يعاقب بالغرامة التي لا تقل عن

ثلاثة آلاف درهم من .... أو استرق السمع في مكالمة هاتفية. ويعاقب الجاني بالحبس مدة لا تقل عن ثلاثة أشهر أو بالغرامة التي لا تقل عن خمسة آلاف درهم إذا أفشى ... أو المكالمة لغير من وجهت إليه ودون إذنه متى كان من شأن ذلك إلحاق الضرر بالغير".

وبمقارنة ما تضمنه قانون مكافحة تقنية المعلومات بخصوص المراسلات الإلكترونية وما تضمنه قانون العقوبات بخصوص استراق وإفشاء الاتصال الهاتفي، يتضح ما يلي:

- إن المشرع الاتحادي لم يعالج تسجيل المحادثات الشفوية التي تجري في مكان خاص، وهو ما ينبغي أن يكون معاقبا عليه، وكان حريا به أن يعاقب على تسجيل هذا النوع من المحادثات مساويا بينه وبين تسجيل المحادثات الهاتفية من حيث التجريم ومن حيث إجراءات الإذن بتسجيلها بوصفها إجراء من إجراءات التحقيق.

- إن المشرع الإماراتي لم يراع التناسق بين المادة (٨) من قانون مكافحة جرائم تقنية المعلومات والمادة (٣٨٠) عقوبات اتحادي؛ حيث عاقب على استراق السمع بالنسبة للمراسلات الهاتفية بالغرامة فقط بينما عاقب على التنصت أو التقاط أو اعتراض المراسلات الإلكترونية بالحبس أو الغرامة أو كليهما (مادة ٨ من القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات)، محققا بذلك حماية أكبر للمراسلات الإلكترونية عن الاتصالات الهاتفية، وهو أمر غير سائغ.

- إن المشرع حقق حماية أكبر للمرسلات الإلكترونية أيضا من ناحية صور النشاط المعاقب عليه؛ حيث عاقب على التنصت والالتقاط

والاعتراض، بينما عاقب على استراق السمع فقط بالنسبة للاتصالات الهاتفية.

- إن المشرع الاتحادي عاقب بصدد المحادثات الهاتفية على إفشاء المكالمة لغير من وجهت إليه ودون إذنه متى كان من شأن ذلك إلحاق الضرر بالغير (مادة ٣٨٠-٢)، ولم يراع ذلك بالنسبة للمراسلات الإلكترونية.

- لم يراع المشرع الاتحادي التناسق الواجب بين المادة ٣٨٠-٢ عقوبات والمادة ٢٤٧ عقوبات، هذه الأخيرة تعاقب على إفشاء سر تضمنته مكالمة تليفونية بالحبس أو بالغرامة إذا وقع الفعل من موظف عام أو مكلف بخدمة عامة، بينما تعاقب المادة ٣٨٠ -٢ عقوبات على إفشاء سر المكالمة دون اشتراط صفة معينة في الفاعل بالحبس مدة لا تقل ثلاثة أشهر أو بالغرامة التي لا تقل عن خمسة آلاف درهم، وكان حريا بالمشرع أن يشدد العقوبة على الفعل الذي يصدر من موظف عام أو مكلف بخدمة عامة عن ذلك الذي يصدر من شخص عادي، وليس العكس.

- إن المشرع الاتحادي لم يورد في قانون مكافحة جرائم تقنية المعلومات أحكاما إجرائية خاصة بالمراسلات الإلكترونية على غرار ما تضمنته أحكام قانون الإجراءات الجنائية بخصوص الاتصالات الهاتفية. فقد نصت المادة (٧٥) إجراءات جزائية اتحادي على أنه " لعضو النيابة العامة أن يفتش المتهم ....وأن يراقب المحادثات السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك". ويُثار التساؤل عن حكم مراقبة المراسلات الإلكترونية: هل نقيم التسوية بينهما؟ وعلى أي أساس قانوني؟ لا شك أن الأمر يتعلق بحرمة الحياة الخاصة وأن نفس المنطق يستوجب أن يكون مراقبة المراسلات الإلكترونية أو تسجيها مشروطا بصدور إذن من النيابة العامة

وفقا لقانون الإجراءات الجنائية الإماراتي. ويجب أن تكون هذه المراقبة أو ذلك التسجيل بعد إذن القاضي الجزئي وفقا للقانون المصري، حيث تنص المادة (٩٤) إجراءات على أنه "لقاضي التحقيق أن يفتش المتهم ....،أن يأمر بمراقبة المحادثات السلكية واللاسلكية وإجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس مدة تزيد على ثلاثة أشهر. وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يوما قابلة للتجديد لمدة أو لمدد أخرى مماثلة". وإذا كان النيابة العامة هي التي تباشر التحقيق، فإن عليها أن تستصدر أمرا مسببا بذلك من القاضي الجزئي. فتنص المادة (٢٠٦) إجراءات مصري على أنه "ويجوز لها أن تضبط لدى مكاتب البريد .... وأن تراقب المحادثات السلكية واللاسلكية وأن تقوم بتسجيل لمحادثات جرت في مكان خاص، متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة لا تزيد على ثلاثة أشهر. ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق ...".

واحتراما لمبدأ الشرعية فإن التنصت على المحادثات الفورية الإلكترونية وتسجيلها لا يقع تحت طائلة التجريم، الأمر الذي يحتاج إلى وجوب سد هذه الثغرة في التشريع المصري (بينما عالجها في دولة الإمارات المشرع الاتحادي في المادة ٨ من القانون رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات). ويبرز ذلك ضعف ما تتمتع به المحادثات الإلكترونية عن طريق الإنترنت من حماية جنائية، وذلك لاختلاف المحادثات الفورية عن

طريق شبكة الإنترنت عن المحادثات الهاتفية، فلا يمكن أن يسري عليها وصف المحادثات الهاتفية على الرغم من أن شبكة الإنترنت تعمل بالاتصال بخط هاتفي. والحقيقة أن هناك طريقان للاتصال بشبكة الإنترنت وبالتالي إجراء محادثات فورية؛ الطريقة الأولى الاتصال المباشر بخط هاتفي يتم توصيله بالجهاز، والطريقة الثانية الاتصال بخط سريع يتصل بالسنترال (هيئة الاتصالات بالإمارات). وحتى في هذه الحالة فإن شبكة الإنترنت تتصل في مرحلة من مراحلها بشبكة الهواتف. ومع ذلك فإن المحادثة بطريق الإنترنت ذات طابع خاص يتميز عن الاتصال الهاتفي وبالتالي لا يمكن أن يسري عليه وصف التجريم الوارد في التجريم سالف الذكر.

لهذا السبب فإن التشريعات الحديثة أدرجت في نصوصها تجريما يسوي بين اعتراض الاتصالات السلكية والإلكترونية كالقانون الأمريكي (٢٥١١, Sec. ١١٩, Part I, Chapter ١٨Title)[1]. بل أكثر من ذلك فإن القانون الأمريكي ينص على تجريم حظر صناعة أو تجميع أو حتى حيازة أو بيع أي وسيلة ميكانيكية أو غيرها إذا كان المتهم عالما بأن الغرض منها هو اعتراض الاتصالات السلكية أو الشفوية أو الإلكترونية. وقد عُني المشرع الأمريكي بتحديد المقصود بالاعتراض بأنه الحصول على محتوى الاتصال السلكي أو الشفوي أو الإلكتروني أي تسجيل الاتصال بشكل غير قانوني[2].

ونظرة إلى القانون المصري نجد أنه لم يتضمن إلاّ نصوصا خاصة

---

(١) a) intentionally intercepts any wire , oral or electronic .connunication

2)) انظر د. شيماء عبد الغني محمد عطاالله، المرجع السابق ص ٢٩٤.

بتسجيل المحادثات الشفوية والهاتفية (سواء أكانت تلك الأخيرة سلكية أم لاسلكية)، مستلزما لهذا التسجيل سبق الحصول على إذن من القاضي الجزئي. فتنص المادة ٢٠٦ من قانون الإجراءات المصري على أنه "ويجوز لها (أي النيابة العامة) ... وأن تراقب المحادثات السلكية واللاسلكية وأن تقوم بتسجيلات لمحادثات جرت في مكان خاص، متى كان لذلك فائدة في ظهور الحقيقة في جناية أو في جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق".

- وجوب صدور إذن قضائي للدخول إلى البريد الالكتروني :

نظرا لحرمة الحياة الخاصة التي يتمتع بها الشخص بالنسبة لبريده العادي، فإنه يتمتع بهذا الحق بالنسبة لبريده الإلكتروني (الإيه ميل). وبناء عليه فإنه يتعين صدور إذن قضائي بالدخول إلى البريد الإلكتروني للمتهم للاطلاع على ما يحتويه من معلومات تفيد في كشف الحقيقة عن جريمة قد وقعت.

وعلى الرغم من أن قانون الإجراءات الجنائية المصري قد تضمن نصا خاصا بالاطلاع وضبط البريد العادي، ومثله فعل قانون الإجراءات الجنائية الاتحادي في الإمارات، فمن الواجب إعمال القواعد المقررة بالنسبة إلى البريد العادي على البريد الإلكتروني.

فقد نصت المادة (٢٠٦) إجراءات مصري على أنه " .. ويجوز لها (أي للنيابة العامة) أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق جميع البرقيات...

ويشترط لاتخاذ إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق. وفي جميع الأحوال يجب أن يكون الأمر بالضبط أو الاطلاع أو المراقبة لمدة لا تزيد على ثلاثين يوما، ويجوز للقاضي الجزئي أن يجدد هذا الأمر مدة أو مدد أخرى مماثلة. ..". وقد قرر المشرع الاتحادي في الإمارات توفير ضمانة "الاختصاص النوعي للنائب العام" عن طريق وجوب صدور إذن من النائب العام وليس من أي عضو من أعضاء النيابة العامة إذا تعلق الأمر بالاطلاع على "جميع المكاتبات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق جميع البرقيات ...".

لذا نرى أنه على الرغم من اختلاف النوعين من المراسلات البريدية والإلكترونية، فإنه نظرا لتعلق الأمر بحرمة الحياة الخاصة، فإنه يتعين أن يدخل المشرع نصا صريحا على سريان نفس الضمانات السابقة وهي المقررة بالنسبة للمراسلات البريدية على المراسلات الإلكترونية.

وقد أدرك القضاء في بلاد أخرى ضرورة التسوية بين البريد العادي والبريد الإلكتروني في الضمانات المتعلقة بالتحقيق، فقضي في الولايات المتحدة الأمريكية ببطلان الدليل المستمد من دخول رجال الضبط القضائي إلى البريد الإلكتروني للمتهم وحصولهم على دليل لإثبات ارتكابه الجريمة، لعدم حصولهم على إذن قضائي بذلك ولعدم توافر رضاء من صاحب البريد نفسه[1].

(١)U.S. c. Maxwell ٤٥MJ ٤٠٦(١٩٩٦): René PEPIN, Le statut juridique du courriel au Canada et aux Etats- Unis, www.lex-electronica.org/ articles/٧٢-٦/pepin.htm

- حالات تفتيش واعتراض المراسلات والبريد الإلكتروني:

أولا- اعتراض وتفتيش المراسلات والبريد الإلكتروني بناء على إذن قضائي:

تقضي القواعد العامة بأنه إذا لم يتوافر إذن قضائي بالتفتيش، فإنه لا يجوز لرجال الضبط القضائي أن يقوموا بهذا الإجراء إلاّ في حالة التلبس. فتنص المادة (٣٤) إجراءات مصري على أنه "لمأمور الضبط القضائي في أحوال التلبس بالجنايات أو الجنح التي يعاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر أن يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية على اتهامه". كما نصت المادة (٤٦) إجراءات مصري على أنه "في الأحوال التي يجوز القبض قانونا على المتهم يجوز لمأمور الضبط القضائي أن يفتشه". أما تفتيش المنازل فإنه يجب أن يصدر به إذن قضائي مسبب – وفقا للقانون المصري بسبب نص الدستور المصري على أن تفتيش المنازل لا يجوز إلا بناء على إذن قضائي مسبب). وبناء عليه لا يجوز تفتيش المنازل بناء على حالة التلبس. أما القانون الإماراتي، فإنه يجيز تفتيش المنازل – بالإضافة طبعا لتفتيش الأشخاص – بناء على حالة التلبس.

بتطبيق ذلك على تفتيش المراسلات الإلكترونية وعلى تفتيش الإيميل، فإننا نلاحظ أن المشرع لم يضع نصا بخصوصها، والأمر – في رأينا – يتراوح بين نظامين يمكن أن يحكما الاطلاع على هذا النوع من المراسلات؛

النظام الأول- يمكن أن نقيس الاطلاع على المراسلات الإلكترونية على الاطلاع على المراسلات البريدية في نظامهما الإجرائي، فيجوز هذا الاطلاع حيث يجوز في حالة المراسلات البريدية ويتم ذلك الاطلاع بنفس الشروط المقررة في الاطلاع على المراسلات البريدية.

النظام الثاني- وهو يستبعد القياس السابق لعدم تعلق الأمر بضبط أو بتفتيش مكتب البريد وهي طرف ثان مكلف بالمحافظة على أسرار المراسلات. ولما كان الأمر لا يتعلق بتفتيش المنازل بل بالضبط والتفتيش في مكان خاص، الأمر الذي يجوز القيام به بناء على حالة التلبس أو إذن النيابة العامة في القانون المصري وكذلك في قانون الإمارات، وذلك ما دامت تلك المراسلات مخزنة في الإيه ميل الخاص بالمتهم.

ونرى أنه يتعين التمييز بين نوعين من التفتيش والضبط ؛ ضبط وتفتيش المراسلات أثناء وقوعها on line وضبط وتفتيش المراسلات المخزنة. في الحالة الأولى يجب أن يقيم المشرع التماثل بين المراسلات "أون لاين" والمكالمات الهاتفية، عندئذ يتعين توافر شرط الإذن القضائي (من النائب العام في الإمارات ومن القاضي الجزئي في مصر). أما في حالة المراسلات المسجلة، فإن قواعد التفتيش العادية هي التي تسري على اعتبار أن الأمر يتعلق بتفتيش الأماكن الخاصة وليس بتفتيش المنازل. وبناء عليه فإنه يكفي توافر حالة التلبس أو صدور إذن قضائي بذلك للقيام بالدخول إلى الإيه ميل الخاص بالمتهم والاطلاع على ما به من مراسلات أو محادثات مسجلة ، وكذلك للاطلاع على ما لدى مزود الخدمات من محتوى تلك الرسائل التي دارت بين المتهم وغيره من أطراف إذا كان الاطلاع عليها يفيد في كشف الحقيقة عن جريمة وقعت بالفعل.

- الجهة المختصة بإصدار إذن تفتيش الكمبيوتر:

قد يقرر المحقق إصدار أمر باعتراض رسائل مرسلة بطريق الكمبيوتر عبر شبكة مغلقة أو عبر شبكة الإنترنت وقد يتعلق الإذن بتفتيش جهاز معين لضبط ما به من بيانات تفيد في كشف الحقيقة.

في الحالة الأخيرة لا يثير الاختصاص بإصدار الأمر مشكلة قانونية، ذلك بسبب تواجد جهاز الكمبيوتر في مكان معين. وحتى لو قرر المحقق أن يضبط تلك البيانات لدى مزود الخدمات، فإن المحقق يكون مختصا وفقا للمادة ١٤١ إجراءات اتحادي إماراتي مادام أن الجريمة قد وقعت في دائرة اختصاصه، فإذا كان الجهاز أيضا يقع في دائرة اختصاصه، فإن الأمر واضح حيث يختص بإصدار الإذن. أما إذا كان الجهاز واقعا في اختصاص محقق آخر غير مختص بالتحقيق في الجريمة، فإن الأول يقوم بإصدار أمر التفتيش ويطلب من الثاني تنفيذ هذا الأمر. وبالنسبة للتعاون بين الإمارات في تنفيذ مثل تلك الأوامر فإن هناك من القواعد التي تحكم مثل هذا التعاون. بخصوص هذا التعاون تنص المادة (١٠٥) إجراءات اتحادي على أنه "مع مراعاة أحكام القانون الاتحادي رقم (١١) لسنة ١٩٧٣ في شأن تنظيم العلاقات بين الإمارات الأعضاء في الاتحاد إذا قُبض على المتهم خارج دائرة المحكمة التي يجري التحقيق فيها، يرسل إلى النيابة العامة بالجهة التي قبض عليه فيها فورا وعليها أن تتحقق من جميع البيانات الخاصة بشخصه، ثم تحيله إلى النيابة العامة بدائرة المحكمة التي يجري التحقيق بها عن طريق السلطات العامة التي يتعين عليها إيصاله بأسرع وقت. فإذا اعترض المتهم على نقله أو كانت حالته لا تسمح بالنقل، يخطر عضو النيابة العامة المحقق بذلك ، وعليه أن يصدر أمره فورا بما يتبع".

ويختلف الأمر لو كان محل الاعتراض والتسجيل يرد على مراسلات في أثناء تبادلها، في هذه الحالة تمر المراسلات عبر شبكة الإنترنت بأكثر من مكان وقد تنتقل عبر شبكة مغلقة بين أكثر من مكان. عندئذ يؤول الاختصاص للمحقق الذي يختص بإجراء التحقيق ، هذا المحقق يكون مختصا

إذا كانت الجريمة قد وقعت في دائرة اختصاصه وفقا لبعض القوانين (مثل قانون الإجراءات الاتحادي في الإمارات: مادة ١٤٢) ويكون مختصا كل محقق وقعت في دائرة اختصاصه الجريمة أو كان المتهم بها مقيما في تلك الدائرة أو تم القبض عليه فيها في تشريعات أخرى (مثل قانون الإجراءات الجنائية المصري : مادة ٢١٧).

ونظرا للطابع الخاص لإجراءات التحقيق في مجال جرائم تقنية المعلومات بسبب أن الاتصالات عن طريق الإنترنت تتعدي أكثر من مكان، فإنه كان من اللازم أن يمتد اختصاص سلطة التحقيق خارج دائرتها، وذلك لمتابعة الرسائل والاتصالات الإلكترونية عبر أكثر من جهاز يصعب أحيانا تحديد مكان تواجدها سلفا. لذا فإن الاختصاص في القانون الأمريكي (القاعدةرقم٤١- أ من قانون الإجراءات الجنائية الفيدرالي) يؤول إلى المحقق الذي في دائرته يتواجد محل التفتيش أي الجهاز[1].

وإذا كان الجهاز مرتبطا بغيره من الأجهزة وكانت بعض تلك الأجهزة تتواجد في خارج اختصاص المحقق الذي يقع في دائرته أحد تلك الأجهزة، فإن اختصاصه بتفتيش الأجهزة المرتبط بالجهاز الأول يمتد إلى غير ذلك من الأجهزة رغم تواجدها في خارج دائرة اختصاصه. لذا كان من الضروري إيراد من النصوص ما ينظم تفتيش الأجهزة المرتبطة ضمن شبكة واحدة وتفتيش الأجهزة المتصلة بشبكة الإنترنت.

غير أنه يتعين التمييز بين الأجهزة المرتبطة بشبكة داخلية أي في داخل البلد الواحد والأجهزة المرتبطة بشبكة عبر الدول كشبكة الإنترنت أو شبكة

---

(1) د. شيماء عبد الغني محمد عطاالله ، المرجع السابق ص ٣٤٤.

أخرى كالتي تربط بين بنوك مختلفة عبر أكثر من دولة.

في الحالة الثانية دون الأولى يتعين احترام سيادة الدول الأخرى وإيجاد من التنظيم ما يكفل التعاون الدولي في إطار مكافحة جرائم الإنترنت، ذلك أنه توجد برامج تسمح بالدخول إلى الأجهزة المتواجدة في خارج البلاد. في هذه الحالة يجب احترام سيادة الدولة إذا ما تتبع المحقق الرسائل الإلكترونية التي تصل إلى أجهزة الكمبيوتر المتواجدة في دولة أخرى، خاصة إذا تعلق الأمر بأجهزة تنتمي إلى إدارات عامة، وهو ما يقتضي فعلا أن تنظم إجراءات التعاون الدولي في هذا الموضوع. غير أننا نعتقد أن المحقق الذي يحصل على دليل من تلك الأجهزة المتواجدة في خارج البلاد دون توافر تلك الاتفاقات الدولية لا يشوب عمله البطلان لهذا السبب، مادامت إجراءات الحصول على إذن قد اكتملت أو توافرت حالة من حالات التلبس وفقا للقانون الداخلي، وذلك بناء على الارتباط الإجرائي.

في هذا الاتجاه نصت المادة ١٧ / أ من قانون الأمن الداخلي رقم ٢٣٩/ ٢٠٠٣ على أنه "يجوز لرجال الضبط القضائي من درجة الضباط - وغيرهم من رجال الضبط القضائي الذين يعملون تحت رئاستهم - أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات متصلة في شبكة واحدة بالنظام الرئيس أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيس"[١].

---

(١)Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponible pour les système initial ."

ثانيا- جواز تفتيش الكمبيوتر استنادا إلى الرضاء:

بالإضافة إلى حالة الإذن وحالة التلبس، من المقرر أنه يجوز تفتيش الأشخاص والأماكن (ما لم يكن المكان مسكنا في القانون المصري) استنادا إلى رضاء صاحب الحق. هذه القاعدة تجد تطبيقا لها في مجال ضبط الدليل الإلكتروني مع بعض أوجه الخصوصية، على ما سيلي؛

صحة التفتيش الصادر صاحب النظام:

تعطي أحكام القضاء كل صاحب حق على النظام أن يرضى بتفتيشه. ولا تستلزم تلك الأحكام أن يصدر الرضاء من صاحب النظام نفسه، بل يكفي أن يصدر من أي شخص يستعمل هذا النظام. لذا فإن المحاكم الأمريكية قد قضت بأن العبرة هي بالاعتياد على استعمال الجهاز وليس بملكية ذلك الجهاز، وبناء عليه قضت بأن الصديقة من حقها أن ترضى بتفتيش جهاز الكمبيوتر الموجود في منزل تسكنه مع المتهم، مادام أنه كان مسموحا لها باستعماله وآية ذلك عدم استعانة صاحبه بكلمة المرور ليختص بفتحه واستعماله، فرضاؤه باستعمالها للجهاز يجعل لها حيازة عليه ومن ثم فإن الرضاء الصادر منها بتفتيش الجهاز يكون فعّالا ومنتجا لأثره[1]. وعلى العكس من ذلك قُضي بأن وجود كلمة السر وضعها صاحب الجهاز تفيد رغبته في الاستئثار بملفات الجهاز وعدم السماع للغير بفتحها، ومن ثم يجوز الاستناد إلى ذلك للقول بعدم فعالية الرضاء بالتفتيش[2]. ويُفهم من ذلك أن أحكام القضاء الأمريكي تعتد بالسلطة الظاهرة على الجهاز وترتب عليه أثرها في فعالية الرضاء في جواز التفتيش. بل لقد ذهبت أحكام القضاء الأمريكي – في حكم Matlock الشهير – إلى جواز صدور الرضاء من

---

(1)United States v. Smith, ٢٧F. Supp. ٢d ١١١, ١٦-١١١٥(C.D.III. ١٩٩٨), www.cybercrime.gov/s&smanual ٢٠٠٢.htm

(2) Trulock v. Freeh, ٢٧٢F.٣d ٣٩١, www.cybercrime.gov/s&smanual ٢٠٠٢.htm

الخليلة التي تساكن المتهم في نفس المنزل حتى ولو كان صاحب الجهاز موجودا واعترض على ذلك التفتيش[1].

ومن مظاهر صحة تفتيش الكمبيوتر المستند إلى الرضاء ذلك الذي يصدر من مدير النظام؛ فالرضاء الصادر من مدير النظام أي المسئول عن تشغيله يعد رضاءً فعّالا في إجازته لذلك التفتيش بدون إذن وبدون حالة التلبس. وقد وضع المشرع الأمريكي بالفعل نصوصا تقرر له حقا في هذا الخصوص وذلك بمقتضى قانون حماية الحق في الخصوصية في مجال الاتصالات الإلكترونيةECPA (المادة ١٨ U.S.C.§§ ٢٧٠١-٢٧١٧).

صحة التفتيش الصادر من رب العمل:

من صور الرضاء الصحيح بالتفتيش ذلك الذي يصدر من رب العمل بالنسبة لأجهزة الشركة أو الجهة التي يمتلكها وكذلك رضاء المدير الذي له حق الإشراف على تلك الشركة. فتستقر أحكام القضاء في أمريكا على فعالية ذلك الرضاء مادام أن الأمر يتعلق بأجهزة العمل[2]. أما القضاء الفرنسي فإنه يكرس مبدأ حق العامل في حرمة حياته الخاصة بالنسبة لمراسلاته الخاصة عبد أجهزة الكمبيوتر ولا سلطة رب العمل في مراقبة تلك المراسلات[3].

توافر الرضاء المفترض استنادا إلى التحذير عن وجود مراقبة:

ومن صور الرضاء المفترض ما يتم تدوينه في تنبيهات تظهر على

---

(١)United States v. Matlock, ٥٩٠F.٢d ٥٣٥(١٩٧٨) ,
www.cybercrime.gov/s&smanual ٢٠٠٢.htm

(٢) انظر على سبيل المثال :
United States of America v. Eric Neil Angevine, ٢٨١F.٣d ١١٣٠ (٢٠٠٢) Briggs v. American Air Filter Co, ٦٣٠F. ٢d ٤١٤, ٤١٨(١٩٨٠):
مشار إليه وغيره من أحكام في : د. شيماء عبد الغني محمد عطاالله ، المرجع السابق ص ٢٣٣.
انظر :
ww.w.phillipsnizer.com/library/alldecisions

(٣) Crim. chamber sociale ٢ oct. ٢٠٠١, www.courdecassation.fr/
انظر لمزيد من التفصيل : مرجع د. شيماء سابق الذكر نفس الموضع

شاشة الكمبيوتر – عند استخدام شبكة الإنترنت – بأن المراسلات يمكن أن تخضع للمراقبة. في هذه الحالة يعتبر استمرار مستخدم الكمبيوتر في استعماله دالا على توافر الرضاء المفترض من جانبه، وتصح المراقبة عندئذ[1]. وقد طبق القضاء الأمريكي تلك الفكرة في مجال مراقبة تليفونات السجن في أثناء محادثات السجناء مع خارج السجن؛ فقضي بأن وضع إدارة السجن لافتة بجوار تليفون السجن بأن المكالمات التليفونية من أجهزة السجن يمكن أن تخضع للمراقبة، يصح الاستناد إليه كدليل على توافر الرضاء الضمني بذلك من جانب مستخدم هذا الهاتف، وتصح بالتالي التسجيلات التي تمت للمحادثات التي تمت عن طريقه[2].

ثالثا- اعتراض وتفتيش الاتصالات الإلكترونية بناء على حالة التلبس:

تقضي القاعدة العامة بجواز تفتيش الأشخاص بناء على حالة التلبس وتجيز كثير من التشريعات تفتيش المساكن بناء على حالة التلبس. أما المراسلات الإلكترونية (محادثات وإيه ميل) فإنه قد سبق القول بأنها تستحق تنظيما خاصا، على اعتبار أنها تختلف عن المحادثات التليفونية وكذلك عن المراسلات البريدية الأمر الذي تفطنت إليه بعض التشريعات كالقانون الأمريكي فضمنت قوانينها نصوصا تنظم هذا النوع من الاتصالات.

وعلى أيه حال فإنه يصعب أن نتصور تواجد حالة التلبس في مجال جرائم تقنية المعلومات وفقا للمادة (٣٠) إجراءات مصري (وفي نفس

(١)United States v. Angevine, ٢٨١F.٣d ١١٣٠, ٣٥-١١٣٤; United States v. Moroe , ٥٢M.J. ٣٢٦, ٣٣٠: www.cybercrime.gov/s&smanual٢٠٠٢.htm

(2) United States v. Amen, ٨٣١F. ٢d ٣٧٣, www.cybercrime.gov/s&smanual٢٠٠٢.htm

معناها تذهب المادة ٤٢ إجراءات إماراتي) التي تنص على حالات التلبس وهي تتبع المجني عليه أو العامة للجاني مع الصياح إثر وقوعها، أو وجود مرتكبها بعد وقوعها بوقت قريب حاملا آلات أو أسلحة أو أمتعة أو أوراق أو أشياء أخرى يستدل منها على أنه فاعل أو شريك أو وجدت به في هذا الوقت آثار أو علامات تفيد ذلك. هذه الحالات للتلبس يصعب توافرها في فرضية الجريمة الإلكترونية، ذلك أن ضبط الجاني وهو يرتكب الجريمة الإلكترونية أمر وإن لم يكن مستحيلا فإنه على الأقل صعب الحدوث، كما أن الأصعب منه أن يضبط الجاني بعد ارتكاب الجريمة ببرهة يسيرة وبه آثار تدل على أنه ارتكبها كفاعل أو كشريك فيها أو أن العامة يتتبعونه بالصياح بعد ارتكابها ببرهة يسيرة، خاصة وأن التداخل في أنظمة الكمبيوتر أو استعمال برامج الاختراق يحتاج وقتا كبيرا حتى يتم اكتشافه ومعرفة القائم بتلك الأفعال. فالجريمة الإلكترونية يرتكبها أشخاص على مستوى عال من المهارة الفنية وهم يستخدمون وسائل فنية متقدمة يحتاج المتخصصون من رجال الضبط القضائي وقتا كبيرا لحل ألغازها ومعرفة مرتكبيها سواء اقتصروا على التداخل والاختراق أو استعانوا بتلك الوسائل لارتكاب جرائم أخرى للاستيلاء على مبالغ نقدية أو بضائع أو لارتكاب جرائم أخرى كجرائم الإرهاب مثلا أو الاتجار في المخدرات أو حيازة صور للأطفال تنافي الآداب. ومن ثم فإنه وإن كانت حالة التلبس تجيز تفتيش الكمبيوتر المتواجد في صحبة المتهم (تفتيش الشخص) أو تفتيشه عندما يتواجد في مسكن (تفتيش المسكن في غالبية التشريعات ماعدا التشريع المصري)، فإن صعوبة توافر حالة التلبس يحدو بنا إلى القول بعدم وجود مجال لتفتيش الكمبيوتر في حالة التلبس في مجال الجرائم الإلكترونية، اللهم

إلاّ في حالات محدودة كما لو تم ضبط جريمة جمركية لها علاقة بالكمبيوتر المتواجد بصحبة الراكب (كما لو تعلق الأمر بحيازته لصور مخلة بالآداب). في هذه الحالة يصح القول بتوافر حالة التلبس وبصحة التفتيش وانقلابه من تفتيش إداري إلى تفتيش قضائي يصح معه تفتيش الكمبيوتر، وقد انتهت أحكام القضاء الأمريكي إلى تلك النتيجة[1].

ومن الجدير بالذكر أن المشرع المصري يعاقب منذ سنة ١٩٩٦ " كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صور محفورة أو منقوشة أو رسومات يدوية أو فوتوجرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت منافية للآداب.. ". وقد أحسن المشرع الاتحادي في الإمارات عندما أدخل نصا – بمقتضى القانون رقم ٢ لسنة ٢٠٠٦- يعاقب فيه " كل من أنتج أو أعد أو هيأ أو أرسل أو خزن بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه المساس بالآداب العامة أو أدار مكانا لذلك". ويعد هذا النص من النصوص الخاصة، ذلك أن قانون العقوبات الاتحادي في الإمارات يتضمن نصا في خصوص الصور المخلة بالآداب منذ سنة ١٩٨٧. فتنص المادة (٣٧٢) عقوبات على عقاب "كل من صنع أو استورد أو صدر أو حاز أو أحرز أو نقل بقصد الاستغلال أو التوزيع أو العرض على الغير كتابات أو رسومات أو صورا أو أفلاما أو رموزا أو غير ذلك من الأشياء إذا كانت مخلة بالآداب العامة . ويعاقب بالعقوبة ذاتها كل من أعلن عن شيء من الأشياء المذكورة". أما عن العقوبة المقررة فإن المشرع قد شدد العقوبة عن تلك الأفعال إذا صدرت بطريق

---

(١)United States v. Roberts, ٨٦F. Supp. ٢d ٦٧٨(٢٠٠٠):
www.cybercrime.gov/s&smanual٢٠٠٢.htm

وسائل العلانية الإلكترونية عن تلك العقوبة المقررة لغيرها من وسائل العلانية والتي تقصدها المادة ٣٦٢ عقوبات اتحادي.

- **ذاتية إجراءات الضبط في مجال الجريمة الإلكترونية:**

تتميز إجراءات الضبط في مجال جرائم تقنية المعلومات ببعض الأوجه الخاصة التي تنفرد بها عن إجراءات الضبط في الجرائم الأخرى. من ذلك ما تضمنته المادة ٥٦ إجراءات فرنسي (المعدلة بالقانون رقم ٥٧٥ لسنة ٢٠٠٤ الصادر في ٢١ يونيه سنة ٢٠٠٤) من أنه يجوز عند القيام بضبط بيانات معلوماتية ضرورية للكشف عن الحقيقة أن يرد الضبط على الدعامة المادية التي سُجلت عليها تلك البيانات أو أن يتم عن طريق نسخ البيانات على دعامة مستقلة[1]، ويتم هذا النسخ في حضور الأشخاص الذين يساعدون في عملية الضبط. ومن الأوجه التي تميز عملية ضبط المعلومات المبرمجة أيضا ما تنص عليه المادة السابقة من جواز أن يقوم القائم بالضبط بمسح المعلومات بعد أخذ نسخة منها[2]. كما أجازت المادة ذاتها لرجل الضبط أن يقوم بحجز الأشخاص الموجودين عند تفتيش أجهزة ومعدات معالجة وتخزين البيانات الوقت اللازم لإتمام عملية التفتيش والضبط[3].

(1) Il est procédé à la saisie des données informatiques nécesaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition'

(2)Si une copie est realisé, il peut être procédé, sur instruction du procureur de la République, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la detention ou l'usage est illégal ou dangéreux pour la sécurité des personnes ou des biens.'

(3) "Si elles sont susceptibles de fournir des renseignements sur les objets, documents et données informatiques saisis, les personnes présentes lors de la perquisition peuvent être retenus sur place par l'officier de police judiciaire le temps strictement nécessaire à l'accomplissement de ces opérations".

الفصل الثالث

ذاتية إجراءات المحاكمة

في مجال جرائم تقنية المعلومات

الأصل أن إجراءات المحاكمة في مجال جرائم تقنية المعلومات تجري على ما تجري عليه تلك الإجراءات في غيرها من الجرائم. فهذه الجرائم تنتمي إلى طائفة الجنح وبالتالي فإن الإجراءات المتبعة هي تلك التي تسري في خصوص الإحالة والاختصاص الذي يؤول لمحكمة الجنح بمحاكمة المتهمين في تلك الجرائم. غير أنه يستحسن أن تخصص دائرة متخصصة في محكمة الجنح لمحاكمة المتهمين بهذا النوع من الجرائم، ذلك أنه من الضروري أن يكون القاضي مدربا على فهم أساليب التقنيات الحديثة حتى يتمكن من أداء رسالته في محاكمة المجرمين بارتكاب هذا النوع المتخصص من الجرائم.

المبحث الأول

الطابع الخاص للاختصاص القضائي

في مجال جرائم تقنية المعلومات

تتميز مسألة تحديد المحكمة المختصة في مجال جرائم تقنية المعلومات بطابع خاص سوف نعرضه فيما يلي من توضيح؛

الطابع الدولي لاختصاص المحاكم في جرائم تقنية المعلومات:

تتميز جرائم تقنية المعلومات عن غيرها من الجرائم في أن لها بعدا مكانيا دوليا، وذلك لوجود الجهاز الذي يتم إدخال المعلومات المؤثمة منه في مكان مختلف عن المكان الذي يتواجد فيه الجهاز الخادم (server) ونظرا لظهور الرسائل المؤثمة في دول العالم المختلفة أي في كل مكان تتواجد فيه أجهزة الكمبيوتر المتصلة بشبكة الإنترنت التي تغطي العالم وبالتالي يمكن قراءة تلك الرسائل.

ويثار التساؤل عن تحديد المحكمة المختصة بمحاكمة المتهم عن الجريمة؛ هل هي المحكمة التي يتواجد في دائرتها الجهاز الذي تم إدخال المعلومات منه أو هي المحكمة التي يتواجد فيها الجهاز الخادم أو أن الاختصاص يؤول إلى كل محكمة في أي دول تظهر فيها تلك الرسائل المؤثمة، كما لو كان الأمر يتعلق بجريمة سب وقذف أو جريمة عرض صور فاضحة أو جريمة تحريض على قلب نظام دولة معينة ...؟

تنقسم التشريعات التي تعرف جرائم تقنية المعلومات إلى نوعين ؛ النوع الأول لم يحدد جهة قضائية مختصة ؟ والثاني حدد تلك الجهة بنصوص

خاصة. إلى النوع الأول ينتمي القانون رقم ٢ لسنة ٢٠٠٦ وإلى النوع الثاني تنتمي تشريعات كثير من الولايات المتحدة الأمريكية على ما سيلي بيانه.

تحديد المحكمة المختصة وفقا للقواعد العامة:

في ظل عدم تناول القانون رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة تقنية المعلومات في دولة الأمارات لمسألة الاختصاص، فإنه لا مناص من اللجوء إلى القواعد العامة في تحديد المحكمة المختصة. وتقضي القاعد العامة التي وضعتها المادة (١٤٢) إجراءات بأن المحكمة المختصة بنظر الجريمة هي تلك التي وقعت الجريمة في دائرتها، وذلك بقولها "يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة".

وبناء عليه فإن القواعد العامة يتعين أن تسري عند محاكمة مرتكب جريمة من جرائم تقنية المعلومات مثله في ذلك مثل أي جريمة أخرى. ومع ذلك فإن تطبيق معيار مكان وقوع الجريمة لا يخلو من بعض الصعوبات القانونية التي تجد تفسيرها في الطبيعة الخاصة للجريمة الإلكترونية. فما هو مكان وقوع الجريمة الإلكترونية (جريمة الكمبيوتر والإنترنت)؟

يلزم بادئ ذي بدء أن نذكر أن هناك طائفتين من جرائم تقنية المعلومات؛ الطائفة الأولى وتضم الجرائم البحتة لتقنية المعلومات والنوع الثاني ويتضمن الجرائم التي تقع بطريق من طرق تقنية المعلومات. تنتمي إلى النوع الأول من الجرائم جريمة التدخل والبقاء في النظام وجريمة إتلاف المعلومات والإخلال بسير النظام ... وتنتمي إلى النوع الثاني جريمة السب والقذف بطريق الإنترنت وجريمة النصب وجريمة غسيل الأموال بالاستعانة بالإنترنت ......

في النوع الأول من الجرائم تقع الجريمة على جهاز معين يتداخل فيه المتهم أو يبقى فيه بطريقة غير مسموح بها، وبالتالي يمكن القول بأن الجريمة تقع في نفس المكان الذي يقع فيه الجهاز المعتدى عليه مادام أن النشاط (الدخول أو البقاء) قد حدث في نفس مكان تواجد الجهاز. بيد أنه قد يحدث أن يكون الدخول أو البقاء عن بعد من جهاز متواجد في مكان آخر. عندئذ يمكن القول بأن الجريمة تحدث في مكان وجود الجهاز المعتدى عليه وفي مكان وجود الجهاز الذي استعان به المتهم للقيام بالنشاط وهو الدخول أو البقاء المؤثم. هذا المكان الثاني قد يقع في نفس دائرة اختصاص المحكمة التي يقع في دائرتها الجهاز المعتدى عليه، عندئذ فلا تُثار مشكلة قانونية. وقد يقع هذا المكان في دائرة اختصاص محكمة أخرى بل قد يقع في خارج البلاد. في هذه الحالة الأخيرة يؤول الاختصاص وفقا لمبدأ الإقليمية إلى محكمة الجهاز المعتدى عليه ومحكمة الجهاز الذي تم منه الدخول أو البقاء بالخارج. في ذلك تنص المادة (١) عقوبات مصري على أن "تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه". كما تنص المادة (٢_ أولا) عقوبات مصري على أن "تسري أحكام هذا القانون أيضا على الأشخاص الآتي ذكرهم: أولا- كل من ارتكب في خارج القطر فعلا يجعله فاعلا أو شريكا في جريمة وقعت كلها أو بعضها في القطر المصري". وفي نفس المعنى تنص المادة (١٦) عقوبات اتحادي على أنه "تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة. ويشمل إقليم الدولة أراضيها وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية والفضاء الجوي الذي يعلوها. وتعتبر الجريمة مرتكبة في إقليم الدولة إذا وقع فيها فعل من الأفعال المكونة لها أو إذا تحققت فيها نتيجتها أو

كان يراد أن تتحقق فيها".

ولا نخال أن الأمر يختلف في حالة زرع فيرس في جهاز أو أكثر حيث إن النتيجة في الجريمة - إذا اعتبرناها من الجرائم الخاصة - تقع بتحقق نتيجة معينة وهي وصول الفيرس إلى الجهاز أو إلى الأجهزة المقصودة. وإذا اعتبرناها جريمة إتلاف لعدم توافر نص خاص، فإن جريمة الإتلاف لا تقع هي الأخرى إلاّ بتحقق الضرر في الجهاز أو الأجهزة المقصودة. وجدير بالذكر أن المشرع المصري لا يعرف حتى الآن قانونا خاصا بجرائم تقنية المعلومات (ماعدا قانون التوقيع الإلكتروني الذي تضمن تجريما خاصا بتعديل المعلومات) وبالتالي يتعين تطبيق القواعد العامة في خصوص جريمة الإتلاف. أما المشرع الاتحادي في دولة الإمارات فقد عاقب على مسح أو حذف أو إتلاف المعلومات (مادة ٦ من القانون رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات).

أما بالنسبة للنوع الثاني من الجرائم والتي تنتمي أصلا إلى الجرائم التقليدية ولكن الجديد فيها أنها تقع بطريق من طرق تقنية المعلومات، نقصد بالإنترنت، فإن الأمر يثير بعض الصعوبات القانونية فيما يتعلق بتحديد المحكمة المختصة. فإذا ارتكب شخص سبا أو قذفا في حق شخص آخر، فإن ذلك قد يقع باستعمال جهازين من أجهزة الكمبيوتر كأحد الطلبة الذي أرسل إلى أحد الأساتذة email باسم أستاذ آخر ذاكرا فيه أنه يعتذر من أنه اقتبس حرفيا بحثا من أبحاثه ؛ فالرسالة التي تضمنت سبا غير علني في حق الأستاذ المعني أرسلت من جهاز معين إلى جهاز المرسل إليه. كما يجب ألاّ ننسى بأن الفاعل قد أرسل الرسالة بطريق الإيه ميل، الأمر الذي يعني بأن الرسالة قد مرت بجهاز خادم يتواجد في خارج البلاد. هذه الصعوبة يزيد منها أن تكون الرسالة قد توافر فيها ركن العلانية أي أرسلت على أحد المواقع التي يمكن أن يزورها أي شخص آخر (جمهور من الناس).

في الفرض الأول الذي لا تتحقق فيه العلانية كما في حالة إرسال

رسالة بالبريد الإلكتروني (الإيه ميل) نتواجد أمام ثلاثة أماكن كمعايير مقترحة للمحكمة المختصة: محكمة الجهاز المرسل ومحكمة الجهاز المستقبل ومحكمة مكان تواجد السرفر (الجهاز الخادم)؛ فبأي معيار نستعين به لتحديد المحكمة المختصة ؟ إذا رجعنا إلى قانون الإجراءات الاتحادي في الإمارات والذي يحدد المحكمة المختصة بمكان وقوع الجريمة، وإذا رجعنا إلى قانون العقوبات الاتحادي الذي يجعل هذا القانون يسري (وبالتالي ينعقد الاختصاص للقضاء الاتحادي) وفقا لمبدأ الإقليمية على الجريمة إذا وقعت في البلاد كلها أو جزء منها، نتبين أن الاختصاص يؤول إلى المحكمة التي يتحقق فيها جزء من الجريمة. وبالتالي فإن جريمة السب غير العلني (عن طريق الإيه ميل) تتحقق في مكان الجهاز المرسل وفي مكان الجهاز المستقبل. أما في حالة السب العلني أو القذف فإن العلانية جزء من الركن المادي وبالتالي فإن التساؤل يثار في هذه الحالة إذا تمت الجريمة عن طريق وضع الرسالة المؤثمة على شبكة الإنترنت كما لو وضعها في أحد المواقع التي يمكن أن يزوروها الجمهور. هل يتحقق ركن من الجريمة في كل مكان في العالم بهذه الطريقة؟ وبالتالي هل ينعقد الاختصاص لكل دولة من دول العالم؟ هل تصبح الجرائم التي تدخل العلانية ركنا فيها جرائم عالمية بهذه الطريقة؟

من الواضح أن هناك تحديا جديدا لمعطيات القانون الجنائي بسبب ظهور وانتشار شبكة الإنترنت، ولعل الذوق القانوني قد يمج أن نعتبر أن الجريمة ذات العلانية كركن فيها يصعب أن نقول في خصوصها أن المحاكم في جميع العالم مختصة بمحاكمة المتهم عنها، مع أن أحكاما للقضاء الفرنسي قد اعتبرت الجريمة مرتبكة في كل مكان تظهر فيه الرسائل المؤثمة محل البث[1]، كما أن أحكاما للقضاء الأمريكي قد قضت أيضا بنفس المعنى[2]. ومن

(1) TGI Paris, ١٣nov. ١٩٩٨, Lionel Thoumyre, Hébergement à l'étranger voie sans issue, www.juriscom.net/int/dpt/dpt٢٨.htm

(2) Edias Software International , L.L.C. et al v. Basis International Ltd. ٩٤٦F. Supp. :٤١٣

مشار إليه في د. شيماء عبد الغني ، المرجع السابق ص ٣٧٤.

الواضح في المثال السابق أن مكان الجهاز الذي حملت منه الرسالة تختص المحاكم فيه بمحاكمة المتهم عن الجريمة التي تضمنتها تلك الرسالة. أما مكان السرفر (المكان الخادم)، فإن القول باختصاص المحكمة الذي يقع في دائرتها هذا الجهاز يؤدي إلى نتيجة يصعب قبولها وهي أن المحكمة التي يقع في دائرتها ذلك الجهاز تختص بمحاكمة المتهمين عن كل الجرائم التي تقع بطريق الإنترنت وذلك بسبب أن الجهاز الخادم يؤدي دورا في نقل الرسالة إلى المرسل إليه، فمرور الرسالة مادام أنه يشكل جزءا في الجريمة فإن الاختصاص ينعقد لمحكمة ذلك الجهاز كما هو الحال في الطرد الناسف الذي يمر في أكثر من دولة أو في دائرة أكثر من محكمة في البلد الواحد لذا كان من الضروري أن ينظم القانون تلك المسألة بنصوص خاصة.

وهناك صعوبة قانونية أخرى تتعلق بالاختصاص في الجرائم التي تشكل العلانية ركنا فيها عندما تتحقق تلك العلانية بطريق الإنترنت: فعندما يضع المتهم رسالته المؤثمة (كالسب أو القذف) أو أي جريمة أخرى قولية تكون العلانية ركنا فيها، على شبكة الإنترنت، فإنه يحقق العلانية بذلك الوضع. وهنا يبرز الطابع الخاص للعلانية عن طريق شبكة الإنترنت والذي يختلف عن العلانية بطرق النشر المعتادة كالنشر في الصحف. فعندما يحدث الإسناد في صحيفة من الصحف فيتم أولا تدوين الكتابة المؤثمة في مطابع الجريدة ثم يأتي بعد ذلك توزيع تلك الجريدة عندما تخرج الصحيفة من هذه المطابع إلى متناول الجمهور في خارجها، عندئذ تتحقق العلانية بإمكان إطلاع الغير عليها بمجرد خروجها من أسوار مطابع الصحيفة. أما انتشارها بعد ذلك من مكان إلى مكان كما لو تم نقلها إلى مناطق البلاد المختلفة، فإنه مجرد تأكيد للعلانية وليس تحقيقا لتلك العلانية التي توافرت بالفعل في أول مرحلة عند خروج الصحيفة. فالصحيفة – حتى تصل ليد القارئ- تمر بمراحل ثلاث قبل وصولها إلى منطقة معينة في البلاد؛ المرحلة الأولى مرحلة الطبع ثم

مرحلة التوزيع ثم مرحلة النقل. في المرحلة الأولى يتحقق الإسناد بدون علانية ويشكل ذلك ركنا في الجريمة، وفي المرحلة الثانية تتحقق العلانية وهي ركن في الجريمة، ومن ثم لا صعوبة قانونية في القول باختصاص المحكمة التي تقع في دائرتها مطابع الصحيفة فهناك قد حدث الإسناد ومنها خرجت الصحيفة موضوعة تحت تصرف الجمهور. أما انتقال الصحيفة من مكان لآخر، فإنه لا يعدو أن يكون أثرا من آثار الجريمة، ومن ثم لا يعطي الاختصاص لكل محكمة في البلاد بسبب ظهور الصحيفة التي احتوت على ألفاظ السباب أو القذف في كل مكان في الجمهور.

غير أننا نرى أن الأمر يختلف في حالة العلانية بطريقة النشر في الصحف عن العلانية بطريق الإنترنت. فعندما يضع الفاعل الرسالة المؤثمة على شبكة الإنترنت فإنه يضعها في مكان وجود الجهاز الذي يستعمله لكي يحملها على الشبكة مباشرة. ومعنى هذا أن الرسالة تظهر في جميع أنحاء العالم في وقت واحد. وهنا يكمن الفارق بين النشر في الصحيفة والنشر بطريق الإنترنت؛ فالصحيفة تظهر في مكان ثم تنتقل إلى مكان آخر، أما عن طريق الإنترنت فإن الرسالة تظهر في جميع أنحاء العالم في وقت واحد. ومعنى ذلك أن العلانية تتحقق في كل بلد من بلدان العالم ، الأمر الذي يمجه الذوق القانوني السليم. ومن هنا كان من الواجب أن يتدخل المشرع ليحدد معيارا للاختصاص يتلاءم مع الطبيعة الخاصة لجرائم الإنترنت[1].

(١) د. شيماء عبد الغني محمد عطاالله، المرجع السابق ص ١.٣٧٥)

المبحث الثاني

الطابع الخاص للمستندات الإلكترونية

كدليل في الإثبات أمام المحكمة

تتميز المستندات الإلكترونية بطابع خاص تنفرد به فيما يتعلق بقوتها الثبوتية أمام المحكمة سواء فيما يتعلق بإثبات أركان الجريمة أو بإثبات الشرط المفترض فيها كما في حالة خيانة الأمانة.

القوة الثبوتية للمستندات الإلكترونية أمام المحكمة الجنائية:

لما كان القاضي الجنائي يتمتع بحرية في تكوين عقيدته، فإنه ليس هناك ما يمنع من أن يستند في تكوين ذلك الاقتناع على مخرجات الكمبيوتر. بيد أن تلك المخرجات سواء كانت بيانات مسجلة في داخل الجهاز أو على ديسك أو شريط ممغنط أو على مخرجات ورقية يصح اعتبارها قرينة تُضاف إلى قرائن أخرى لكي تكون اقتناع القاضي الجنائي، ذلك أن تلك المخرجات يمكن التلاعب فيها وليست من القوة بحيث يصح اعتبارها دليلا وحيدا يسند الحكم الصادر بالإدانة. ويطرح ذلك مسألة القوة الثبوتية لمخرجات الكمبيوتر أمام القاضي الجنائي، أما أمام القاضي المدني فإن تلك المخرجات تتعارض مع المحررات التقليدية ومن ثم فإنه يصعب الاستناد إليها ، إلاّ إذا صدر قانون ينظم تلك المسألة في الموضوعات المدنية.

وإذا كانت القوة الثبوتية للمستندات الإلكترونية أمام القاضي الجنائي في التشريعات اللاتينية يعتورها أوجه من الضعف، فإن تلك المستندات كانت مجردة أصلا من القوة الثبوتية أمام القاضي الجنائي في التشريعات الانجلوأمريكية بسبب أن تلك التشريعات تعتنق نظام الإثبات

المقيد، ولم تكن مخرجات الكمبيوتر قد نظمها القانون في تلك التشريعات. هذه الطائفة من التشريعات لم تكن تقبل مخرجات الكمبيوتر أمام القاضي الجنائي إلاّ إذا كانت مشفوعة بشهادة صاحب الجهاز أو مدير النظام أو المسئول عنه[1].

القوة الثبوتية للمستندات الإلكترونية وفقا للقانون المدني:

إذا كانت المستندات الإلكترونية أمام القاضي الجنائي الذي يتمتع بحرية في مجال الإثبات تثير صعوبات قانونية، فإن تلك الصعوبات تزداد من الناحية المدنية في إثبات الالتزامات التي يحيطها المشرع بضمانات منها ضرورة توافر الدليل الكتابي ومنها أن يكون موقعا عليه من المدين بالالتزام. هذه القواعد المدنية في الإثبات قد يطبقها القاضي الجنائي عندما يتعرض لوجود ولإثبات الشرط المفترض في الجريمة إذا كان هذا الشرط متميا إلى القانون المدني كعقود الأمانة في جريمة خيانة الأمانة.

من الجدير بالذكر أن مسألة القوة الثبوتية لمخرجات الكمبيوتر تثير كبر وأعم وهي مسألة القوة الثبوتية لوسائل التكنولوجيا الحديثة التي القاضي يتردد في قبولها بسبب اختلاف تلك الوسائل عما نظمه القانون من وسائل تقليدية في الإثبات وهي المحررات الصادرة عن شخص معين وليس عن آلة والموقعة منه وليست خالية من التوقيع كما هو الحال في تلك المحررات. لذا لا تزال المحاكم في كثير من الدول تتردد في قبول الفاكس كوسيلة من وسائل الإثبات في المواد المدنية لخلوه من توقيع الشخص الصادر منه.

---

(١) انظر لمزيد من التفصيل : د. شيماء عبد الغني محمد، المرجع السابق ص ٣٨٧.

ولكن نظرا لتعاظم دور مخرجات الكمبيوتر بدأت تلك التشريعات في الاعتداد بالقوة الثبوتية لمخرجات الكمبيوتر ولكن بشروط منها أن يعمل النظام بصورة سليمة وأن يكون استخدامه قد جرى على الوجه الصحيح وأن يتوافر في المستند الإلكتروني الشروط الأخرى المتطلب توافرها في المحررات الكتابية التقليدية. بل إن بعض التشريعات تتطلب للاعتداد بها أن يعززها شهادة أحد الشهود(1). والحق أن شرط التوقيع يجعل الاعتداد بالمستندات الإلكترونية أمام القاضي الجنائي أمرا صعبا، ذلك أن المحررات التقليدية يتعين للاعتداد بها أن تكون موقعة من الشخص الصادرة منه، كما أن شرط وجوب تعزيزها بشهادة أحد الشهود يبرز ضعف قيمتها في الإثبات إذا لم يتوافر معها دليل آخر.

ومما يعكس تردد القضاء في قبول المستندات الإلكترونية في الإثبات ما قضت به المحاكم المدنية من أن المعلومات التي ترد بالبريد الإلكتروني (الإيه ميل) لا يتوافر فيها شرط تحديد صاحب تلك الرسالة(2). ولكن إذا توافر من الظروف ما يقطع بتحديد صاحب الرسالة فإن تلك المحاكم قد قبلتها في الإثبات(3).

ولا يحول ذلك دون أن هناك اتجاها متناميا في التشريعات الحديثة بدأ يعترف بالمستندات الإلكترونية بوصفها محررات لها قوة في الإثبات على قدم المساواة مع المحررات التقليدية. فقد عرف المشرع المصري بمقتضى القانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الإلكتروني الكتابة الإلكترونية

---

(1) Yves Robillard, La prevue des communications à l´ère économique: www.avocet.qc.ca/affaires/iitechno.htm
(2) Unitted States v. Jackson, ٢٠٨F. ٣d ٦٣٣(.(٢٠٠٠
(3) United States v. Simpson , ١٥٢F. ٢d ١٢٤١((١٩٩٨

بقوله "كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك" ، كما عرف المحرر الإلكتروني بأنه "رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى مشابهة".

غير أن التشريعات وهي تعترف بالمحررات الإلكترونية تضع شروطا تؤدي في الغالب إلى عدم الاعتداد بها أو إضعاف قوتها الثبوتية بشكل ملحوظ ؛ ذلك أنها تشترط توافر نوع من التوقيع هو التوقيع الإلكتروني الذي قلما يتوافر في العمل. فقد عرّف قانون التوقيع الإلكتروني في مصر هذا النوع من التوقيع بأنه "ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره". وقد وضع هذا القانون السابق شروط الاعتداد وهي: (أ) ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره ، و(ب) سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني (جـ) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني. ومن الواضح أن الشرط الأول يصعب تحققه في مجال التعاملات الإلكترونية، ومن هنا ظهرت فكرة التشفير التي لا تزاد في بداية ظهورها.

وقد اعتد المشرع الاتحادي في دولة الإمارات بالمستند الإلكتروني وعرفه في القانون رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات بأنه "سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن

فهمه". وقد اعتد المشرع الاتحادي بالمستند الإلكتروني وعاقب على تزويره دون أن يسبق تلك الخطوة بتنظيم قوته في الإثبات، سواء في المواد الجنائية أو في المواد المدنية، الأمر الذي كان حريا بالمشرع أن يفعله قبل أن يعاقب على التزوير في هذا النوع من المستندات. فالمادة (٤) من القانون رقم ٢ لسنة ٢٠٠٦ آنف الذكر تعاقب على هذا التزوير بقولها "يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفا به قانونا في نظام معلوماتي. وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر. ويعاقب بالعقوبة المقررة لجريمة التزوير حسب الأحوال من استعمل المستند المزور مع علمه بتزويره".

غير أن الجديد في قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات أنه اعترف بالمستند الإلكتروني حتى قبل أن يتم إخراجه على مطبوع ورقي أي وهو لا يزال مخزنا أو على دعامة إلكتروني بقوله "سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه".

وعلى أية حال فإن صدور القانون رقم ٢ لسنة ٢٠٠٦ يفتح الباب للاعتداد بالمستند الإلكتروني بحيث يكون له قوة في الإثبات مثله في ذلك مثل المحررات التقليدية. غير أن هذا القول في حد ذاته ينطوي على إضعاف للقوة الثبوتية لهذا النوع من المستندات، ذلك أنه يتطلب في المستند الإلكتروني نفس الشروط الواجب توافرها في المحررات الكتابية التقليدية

وهي التوقيع حتى يكون مقبولا بشكل كامل كدليل كتابي على الـرغم مـن أنه مكتوب بشكل إلكتروني على دعامة إلكترونيـة، ويتطلـب لكـي يكـون معتدا به كمبدأ ثبوت بالكتابة أن يكون مكتوبا بخـط يـد المـدين بـالالتزام ، الأمر الذي لا يتوافر أيضا بالنسبة للمستند الإلكتروني. لذا فإنه من الواجب إيجاد من النصوص الخاصة ما يأخذ في الاعتبار الطبيعة الخاصـة لهـذا النـوع من المستندات. ومن الخطوات التي بدأت في هذا الاتجاه الأخذ بفكرة التوقيع الإلكتروني ولكن يبقى أن نعمم تلك الوسيلة التي تنتمي أصلا إلى الوسائل التقليدية بحيث تصبح معتادة في مجال التعاملات الإلكترونية.

المبحث الرابع

الاختصاص الدولي بمحاكمة المتهمين

بجرائم الإنترنت

- البعد الدولي لجرائم الإنترنت:

تختلف الجرائم التي تقع بطريق الإنترنت عن غيرها من الجرائم من ناحية مكان ارتكاب الجريمة ، حيث تقع الجريمة في أكثر من دولة . وبناء عليه ينعقد الاختصاص لكل دولة لمحاكمة المتهمين بجرائم الكمبيوتر . ويُعد ذلك تطبيقا لمبدأ الإقليمية ، حيث يقع جزء من الجريمة في كل دولة .

- التفرقة بين جرائم الإنترنت والجرائم الدولية:

لا يتحقق للجرائم التي تقع بطريق الإنترنت صفة الجرائم الدولية ، ذلك أن الجريمة الدولية لها تعريف لا يسري على هذا النوع من الجرائم. فالجريمة الدولية تقع اعتداء على مصلحة جوهرية للمجتمع الدولي ، مثل الجرائم ضد الإنسانية وجريمة إبادة الجنس البشري وجريمة الاتجار بالرقيق[1] . وعادة ما تتعرض الاتفاقيات الدولية لتحديد هذه الجرائم الدولية. أما الجرائم التي تقع بطريق الإنترنت، فإنها تكتسب البعد الدولي بسبب وقوع جزء منها في

---

(١) تضمن الإعلان العالمي لحقوق الإنسان الصادر من الأمم المتحدة في ١٠ ديسمبر سنة ١٩٤٨ نص المادة ٤ منه التي تحظر استرقاق أحد أو استعباده وتحظر الرق والاتجار بالرقيق بجميع صورهما . وكذلك تضمن العهد الدولي للحقوق المدنية والسياسية الصادر في ١٦ ديسمبر سنة ١٩٦٦ نصا بهذا المعنى (مادة ١/١٨).وقد وقعت الدول اتفاقية خاصة بالرق في جنيف في ٢٥ سبتمبر سنة ١٩٢٦ نافذة في ٧ ديسمبر سنة ١٩٥٣. ويُضاف إلى ذلك الاتفاقية التكميلية لإبطال الرق وتجارة الرقيق والأعراف والممارسات الشبيهة بالرق الموقعة في جنيف في ٧ سبتمبر سنة ١٩٥٦ . كما أقرت الجمعية العامة للأمم المتحدة اتفاقية حظر الاتجار بالأشخاص واستغلال دعارة الغير بقرارها الصادر في ٢ ديسمبر سنة ١٩٤٩ .

أكثر من دول. ولا يرجع ذلك إلى طبيعة الجريمة ذاتها ، بل إلى أسلوب ارتكابها ، حيث تقع بطريق شبكة الإنترنت ، الأمر الذي يحقق عالمية تلك الجريمة[1]. ولكن ذلك لا يحول دون وقوع بعض الجرائم الدولية بطريق الإنترنت ، مثل جرائم الإرهاب وجرائم التحريض على الجرائم الدولية بوجه عام ، كالتحريض على إبادة الجنس البشري .

يترتب على هذا الاختلاف بين جرائم الإنترنت والجرائم الدولية اختلاف محاكمة المتهمين بالنوع الأول من الجرائم عن المتهمين بالنوع الثاني من تلك الجرائم . فالطبيعة الدولية للجرائم الدولية تستدعي محاكمة دولية يشترك فيها قضاة دوليون ، على غرار محاكمة مجرمي الحرب في يوغسلافيا سابقا . أما في حالة جرائم الإنترنت التي لا تكتسب الطبيعة الدولية ، فإن المتهمين بها يحاكمون أمام محاكم وطنية طبقا للقانون الوطني وبإجراءات تتم وفقا لهذا القانون وليس وفقا للقانون الدولي .

- ضرورة التعاون الدولي لمكافحة جرائم الإنترنت :

يستدعي البعد الدولي لجرائم الإنترنت أن يتم تنظيم التعاون الدولي في سبيل مكافحة جرائم الإنترنت. ومن مظاهر هذا التعاون الدولي المساعدة الدولية بين أجهزة الشرطة الدولية " الإنتربول " لمتابعة المجرمين والقبض عليهم . كما يستدعي ذلك أيضا تنظيم التعاون على مستوى أجهزة التحقيق "النيابة العامة " وأجهزة المحاكمة، بحيث يتم الاعتداد بأعمال التحقيق والمحاكمة التي تجري في دولة معينة في الدول الأخرى في مجال هذا النوع من الجرائم.

(١) د. عمر الفاروق الحسيني ، المرجع السابق ص ١٣٩ .

كما أن مستوى التعاون يمكن أن يرقى إلى مستوى التشريع في الدول المختلفة بحيث يتم إيجاد مستوى معين من الاتفاق في تجريم الأفعال . فلا يستفيد المجرم من تسامح بعض البلاد التي لا يوجد فيها نص بتجريم سلوك معين لكي يقوم باستغلال شبكة الإنترنت في ارتكاب هذه الجرائم في بلاد أخرى.

يبقى أنه من الطبيعي أن تبقى أوجه للاختلاف بين الدول لاختلاف ثقافتها وعاداتها وتقاليدها ومستواها السياسي ، ومع ذلك فإن الاتفاقيات الدولية يجب أن تتكفل بإيجاد مستوى من القيم المشتركة بين الدول . وهذا يقودنا إلى القول بأن جرائم الإنترنت تتجه نحو اكتساب الطبيعة الدولية أي أنها في طريقها لأن تصبح جريمة دولية ، مادامت الدول المختلفة سوف تتفق على تجريم ما يعتبر منها ماسا بقيم إنسانية مشتركة للجماعة الدولية .

- مشكلات التعاون الدولي في خصوص جرائم الإنترنت:

تثور بعض المشكلات القانونية التي من شأنها أن تحد من التعاون الدولي في مجال مكافحة الجرائم التي تقع بطريق الإنترنت . وترتبط هذه المشكلات ببعض العقبات العملية والقانونية التي تظهر في مجال جرائم الكمبيوتر . من هذه الصعوبات ما يلي:

١ - صعوبة معرفة فاعل الجريمة أحيانا.

٢ - وقوع الجريمة في خارج الدولة التي يحدث فيها البث

٣ - عدم اتفاق الدول على تجريم بعض الأفعال

٤ - عدم وجود اتفاقيات دولية لتسليم المجرمين في مجال جرائم الكمبيوتر والإنترنت

٥ – عدم اعتبار جرائم الكمبيوتر والإنترنت من الجرائم الدولية .

وسوف نقوم بتوضيح تلك الصعوبات فيما يلي :

١ – صعوبة معرفة الفاعل أحيانا :

– كثيرا ما يتخذ الفاعل احتياطات تكفل صعوبة التوصل إلى الكشف عن شخصيته وذلك بخصوص البث عبر شبكة الإنترنت . فأحيانا يقوم المتهم بإرسال رسائل تشكل جرائم من جهاز عمومي بحيث يصعب معرفة مرسل تلك الرسائل . وقد يستخذ إجراءات غرضها التمويه على المرسل إليه بقصد إخفاء شخصيته ، فيتدخل في موقع شخص آخر أو جهة أخرى ويبث من خلال موقعها صورا فاضحة أو أقوالا مسيئة لصاحب الموقع أو لأشخاص آخرين . وقد يعمد الفاعل إلى خلق موقع باسم شخص مجهول ويقوم ببث رسائل أو صور معاقب عليها.

وتواجه السلطات صعوبات كبيرة أحيانا في اقتفاء أثر المجرمين الذين يستعينون بشبكة الإنترنت لارتكاب جرائمهم ، نظرا لما يتميزون به من ذكاء وخبرة كبيره في الاستعانة بالتقدم التقني في مجال الكمبيوتر والإنترنت .

وتثير مشكلة تحديد الفاعل مدى مسئولية مقدم الخدمات provider والذي يتفق معه بعض الأشخاص على فتح صفحة لهم على شبكة الإنترنت ، إذا ورد بتلك الصفحة ما يشكل فعلا يعاقب عليه القانون . ذلك بأنه قد يتفق مع صاحب الصفحة على محتويات معينة ، وبالتالي فإن علمه بما يُنشر على الشبكة يتوافر . وقد لا يعلم بذلك مسبقا ولكن يعلم به بعد ذلك ويستمر في السماح بنشر ما ينطبق عليه وصف الجريمة . عندئذ فإن مسئوليته الجنائية تقوم .

أما بالنسبة للنظام الذي يخضع لـه مـزود الخـدمات provider ، فـإن الرأي يتجه في فرنسا لإخضاعه لنظام المسئولية الجنائية لرئيس التحرير، وهو النظام الذي ينفرد في هذا البلد بخصائص تميزه فيما يتعلق بقرير المسئولية عند عدم معرفة الفاعل(١). هذه القرينة للمسئولية المفترضة لرئيس التحرير لم يعد يعرفها القانون المصري منذ الحكم بعدم دستورية الفقـرة الأولى مـن المـادة ١٩٥ من قانون العقوبات(٢).

٢ - وقوع الجريمة في خارج الدولة التي يحدث فيها البث:

- تقع الجريمة - في الوضع العادي للأمور - في نفس المكان الذي يقـع فيه الفعل ، أي تقع النتيجة في نفس المكان الذي يقع فيه النـشاط . بيـد أنـه بالنسبة لجرائم الكمبيوتر والإنترنت ، تقع الجريمـة في كـثير مـن الأحيـان في مكان آخر غير مكـان البـث . فـإذا أرسـل المـتهم الرسـالة المؤثمـة بطريـق الكمبيوتر من دولة معينة إلى شخص آخر في دولة أخرى ، فإن النشاط يظهر في الخارج وليس في دولة الإرسال. صحيح أن هذا الظهـور لـيس معنـاه أن النشاط لم يقع في دولة الإرسال ، ولكنه يـؤدي إلى عـدم علـم الـسلطات في الدولة التي يرسل منها المتهم تلك الرسائل بما قام به هذا المـتهم مـن أفعـال يعاقب عليها القانون . وبالتالي يؤدي ذلك إلى عدم الإسراع في اتخاذ ما يلزم من إجراءات الاستدلال والتحقيق التي لها أثر رادع بالنسبة لارتكاب الجرائم من هذا النوع . وجدير بالذكر أن تأخير القيـام بتلـك الإجـراءات لـه أثـره السلبي على تجميع الأدلة ضد المتهم . وكل ذلك من شأنه

إعاقة مكافحة هذا النوع من الجرائم.

وبالمثل فإن المتهم قد يقوم بإرسال أوامر بطريق الإنترنت من بلد معين إلى البنك الذي يقع في بلد آخر - وذلك بعد التعرف على كلمـة المـرور إلى

---

(١) د. جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، دار النهضة العربية ، ٢٠٠١ ، ص ١٢١ .

(٢) القضية رقم ٥٩ لسنة ١٨ ق. دستورية ، جلسة ١/٢/١٩٩٧ .

نظام البنك - لكي يتم تحويل مبلغ معين من البنك إلى بلده أو إلى بلد ثالث[1]. وفي الحالة الأولى ، تقع الجريمة في البلد الذي صدر من الأمر باعتبار أن ذلك جزء من النشاط ، سواء اعتبرنا هذا النشاط نصبا أو اعتبرناه من قبيل السرقة . ونحن نميل إلى اعتباره نصبا . وفي الحالة الثانية التي يتم تحويل مبالغ إلى بلد ثالث تقع الجريمة في بلاد ثلاثة : البلد الأولى ؛ وهي التي يصدر منها الأمر ، والبلد الثاني وهي البلد الكائن فيها البنك ، والبلد الثالث هي التي وصلت إليها المبالغ باعتبار أن التسليم جزء من جريمة النصب . وهنا تظهر أهمية تكييف الفعل على أنه نصب لا سرقة، حيث إنه في حالة السرقة لا يمكن تتبع الأمر فيها إلاّ باعتباره إخفاء لأشياء مسروقة.

وقد أدى ذلك إلى تجريم بعض الدول لبعض صور من النشاط التي من شأنها أن توسع من اختصاص قضائها في خصوص جرائم الكمبيوتر . من ذلك قانون جرائم الكمبيوتر لولاية Tennessee الأمريكية الذي ينص على عقاب كل من تحصل على أو أخفى أو استعمل أو ساعد شخصا آخر في الحصول على أو إخفاء أو استعمال كل ما ينتج عن الجرائم المشار إليها في هذا القانون وهي التداخل بقصد الحصول على أموال للغير أو تغيير أو الإضرار بالنظام[2].

أكثر من ذلك فقد عمد المشرع في ولاية Tennessee إلى مد اختصاص محاكم الولاية بخصوص جرائم الكمبيوتر . فقد نص قانون جرائم الكمبيوتر

---

(١) د. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، المرجع السابق ، ص ١٤١ .

(٢) انظر فصل violations - penalities من قانون جرائم الكمبيوتر في ولاية Tennessee الأمريكية:

" (e) Whoever receives, conceals, uses , or aids another in receiving , concealing or using any proceeds resulting from a violation of either subsection (a) or subdivision (b)(2) , knowing the same to be proceeds of such violation , or whoever receives, conceals , uses , or aids another in receiving , concealing or using , any books , records , documents , property , financial instrument, computer software , program, or other material , property , or objects , knowing the same to have been used in violating either subsection (a) or subdivision (b)(2) violates this subsection and is subject to the penalties of section 39 - 14 - 105 " .

في الفصل المتعلق بالاختصاص على وقوع الجريمة في كل مكان يقع فيه فعل من الأفعال المعاقب عليها . كما نص على وقوع الجريمة في كل مكان يسيطر فيه المتهم على مال متحصل من جريمة من جرائم الكمبيوتر أو يتواجد هذا المال في حيازته . كما تقع الجريمة - وفقا لهذا القانون - في كل مكان يحوز فيه المتهم كتبا أو تسجيلات أو وثائق أو أموال أو أوراق مالية أو برامج كمبيوتر أو أي أشياء مادية استخدمت في ارتكاب جريمة من جرائم الكمبيوتر . بل إن هذا القانون قد وسّع من اختصاص محاكم الولاية لكي يمتد إلى جرائم الكمبيوتر إذا وقع فعل التداخل على إقليم الدولة أو تم خارج الدولة ولكنه وقع عبورا بإقليم الدولة ، سواء تم هذا التداخل بأسلوب سلكي أو لاسلكي بطريق الموجات الكهرومغناطيسية أو المايكروويف أو بأي أسلوب آخر من أساليب الاتصال[1].

وقد اتجه المشرع في إنجلترا تلك الوجهة عندما خول الاختصاص بمحاكمة المتهمين بجرائم الكمبيوتر إذا وجدت صلة بين الجريمة والإقليم البريطاني significant link كما لو بدأت الجريمة في إنجلترا أو كان محلها كمبيوتر متواجد في الأراضي البريطانية (الفصل الخامس من قانون إساءة استعمال الكمبيوتر Computer Misuse Act لسنة ١٩٩٠).

٣ - عدم اتفاق الدول على تجريم بعض الأفعال:

- تختلف الدول في نظرتها إلى بعض الأفعال ؛ فتعاقب عليها بعض الدول

(١) انظر فصل venue من قانون جرائم الكمبيوتر في ولاية Tennesse الذي نصّ على :
" For the purposes of venue under the provisions of this part, any violation of this part shall be considered to have been committed : 1- in any county in which any act was performed in furtherance of any transaction violating this part; 2- in any county in which any violator had control or possession of any proceeds of the violation or of any books , records , documents, property, financial instrument, computer software , computer program or other material , objects or items which were used in furtherance of the violation, and 3 - In any county from which, to which or through which any access to a computer , computer system, or computer network was made , whether by wire, electromagnetic waves , microwaves or any other means of communication ".

بوصفها من الجرائم التي ينظر إليها بعين الخطورة ، وتتسامح في خصوصها دول أخرى باعتبارها من مظاهر التعبير عن الرأي الذي تكفله الدساتير في هذه الدول. من تلك الأفعال التي تختلف في شأنها النظرة بين الدول عرض الصور الجنسية الفاضحة ، والعيب في الأديان ، وانتقاد نظام الحكم الداخلي . فبينما تتساهل بعض الدول في خصوص عرض الصور الخليعة ، فإن دولا أخرى تتشدد في حظرها . وفي حين تعاقب بعض الدول على انتقاد الأديان ومهاجمة الرسل والآلهة ، تعتبر دول أخرى أن ذلك من الجرائم المعاقب عليها بالإعدام . وبالمثل فإن هناك من الدول ما يعتبر مهاجمة نظام الحكم من جرائم أمن الدولة ، بينما تعتبر دول أخرى أن ذلك من مظاهر حرية الرأي التي تكفلها الدساتير ويعتز بها الرأي العام داخل تلك الدول.

ويؤدي غياب الاتفاق على الأفعال التي تعتبر جرائم وتلك التي تفلت من التجريم إلى عدم وجود إجماع على مكافحة تلك الأفعال على مستوى الدول المختلفة. ومن شأن ذلك أن يؤدي إلى عدم التعاون الدولي في مكافحة هذا النوع من الأفعال الذي لا يعتبر من الجرائم في الدول التي يقوم المتهم فيها بالنشاط ولكنها تحدث أيضا في دول أخرى يعاقب عليها قانون العقوبات ومع ذلك ينجو الفاعل من العقاب ويستمر في إرسال تلك الرسائل من تلك الدول.

٤ - عدم وجود اتفاقيات دولية بخصوص جرائم الكمبيوتر والإنترنت:

-لم تجتمع الدول على التوقيع على اتفاقية واحدة لمكافحة جرائم الكمبيوتر والإنترنت، والأمر متروك في غالبية الأحوال إلى الاتفاقيات الثنائية التي تبرم بين الدول والتي تتناول جرائم مختلفة ، ينتمي إليها البعض من جرائم الكمبيوتر ولا ينتمي إليها البعض الآخر. ويبرهن ذلك على الحاجة

إلى اتفاقيات ثنائية واتفاقيات جماعية لمكافحة الجرائم التقليدية التي تقع بطريق الكمبيوتر والإنترنت وكذلك مكافحة الجرائم الخاصة التي لا تقع إلاّ بطريق الكمبيوتر والإنترنت.

٥ - عدم اعتبار جرائم الكمبيوتر والإنترنت من الجرائم الدولية :

- لم تستشعر الدول أن جرائم الكمبيوتر والإنترنت قد وصلت إلى مرتبة الإخلال بالقيم العالمية المشتركة على النحو الذي يتوافر بالنسبة لغيرها من الجرائم مثل جرائم الحرب والجرائم ضد الإنسانية . ولذلك فإنه لا توجد اتفاقيات دولية مشتركة تعالج تلك الطائفة من الجرائم و لم تعالجها الأمم المتحدة في قراراتها . كما أن العرف الدولي لم يقر اعتبار مثل هذه النوعية من الجرائم ضمن الجرائم الدولية.

مع ذلك فإن هناك مقدارا من الاتفاق بين الدول المختلفة بدأ يتشكل نحو إعداد اتفاقيات دولية مشتركة تحرم استغلال الأطفال جنسيا كعرض صور جنسية Child Pornography لهم وممارسة الشذوذ الجنسي معهم Pedophilia عن طريق الإنترنت . ومن الواضح أن ذلك من شأنه أن يزيد التعاون الدولي في مجال مكافحة جرائم الكمبيوتر والإنترنت[1] .

والجدير بالذكر أن هناك من الاتفاقيات الدولية ما يتعلق بالاتجار بالمخدرات (اتفاقية سنة ١٩٦١) وبغسيل الأموال وكذلك التعامل في الصور والمنشورات الفاضح obscene)agreement for the Suppression of the Circulation of Obscene Publications of 4 May 1910 and Amended by the Protocole of 4 May 1949) [2] .

---

(١) انظر

John T. Soma, Thomas F. Muther, Jr. Heidi M. L. Brissette, id, p. 333.

(٢) انظر :

Bassiouni , " A draft International Criminal Code and Draft Statute for an International Criminal Tribunal , Martinus Nijhoff Publishers , Boston 1987 , p.439.

- أهمية تحديد مكان وقوع الجريمة بالنسبة للاختصاص بالمحاكمة :

من المعلوم أن لتحديد مكان وقوع الجريمة أهمية واضحة لمعرفة المحكمة المختصة . فالمحكمة المختصة لمحاكمة المتهم بارتكاب جريمة من جرائم الإنترنت هي تلك المحكمة التي وقع الفعل أو جزء منه في دائرة اختصاصها . وليس ظهور أثر من آثار الجريمة على شبكة الإنترنت مؤداه اختصاص محاكم جميع الدول بمحاكمة المتهم بها . ذلك أن العبرة بتحديد الاختصاص القضائي هو بأركان الجريمة وليس بآثار تلك الجريمة أو بالمكان الذي يظهر فيه دليل من أدلتها.

وتقضي القواعد العامة في الاختصاص القضائي بأن المحكمة المختصة بمحاكمة المتهم بالجريمة تتحدد وفقا لمكان وقوع الجريمة أو مكان القبض على المتهم أو مكان إقامة هذا الأخير[1]. ويتوقف تحديد معيار الاختصاص وفقا لاتجاه المشرع داخل الدولة. فمن الدول ما تأخذ بمعيار مكان وقوع الجريمة فقط ، مثل دولة الإمارات العربية المتحدة . فتنص المادة ١٤٢ من قانون الإجراءات الجزائية الاتحادي بدولة الإمارات العربية المتحدة على أنه " يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة" . ومن الدول ما تأخذ بمعيار مكان القبض على المتهم أو محل إقامته أيضا بالإضافة إلى المعيار الأول ، مثل جمهورية مصر العربية. فتنص المادة ٢١٧ من قانون الإجراءات الجنائية المصري على أنه "يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة أو الذي يقيم فيه المتهم ، أو الذي يقبض عليه فيه ".

وبالنسبة للدول الأوربية يختص قضاء كل دولة أوربية بموطن المدعى

---

(١) د. عبد الرءوف مهدي ، شرح القواعد العامة للإجراءات الجنائية ، دار النهضة العربية ، الجزء الثاني ، ٢٠٠٠ ص ٦٥

عليه ، وذلك وفقا لاتفاقية بروكسل وموجانو Bruessels and Lugano Conventions [1]. فإذا كان المتهم يقيم في أي دول من دول الاتحاد الأوربي، فإن ذلك يسمح بمحاكمته في إنجلترا مثلا وفقا للقانون الإنجليزي . وهذا مشروط طبعا بشرط عدم ازدواجية المحاكمة.

- أهمية تحديد مكان وقوع جرائم الإنترنت بالنسبة للاختصاص بالمحاكمة :

لما كان مكان إقامة المتهم غير معلوم في حالات كثيرة وبخاصة في جرائم الكمبيوتر والإنترنت ، فإن قانون إساءة استعمال الكمبيوتر في إنجلترا لسنة ١٩٩٠ (Computer Misuse Act 1990) قد تضمن نصا يعطي الاختصاص للمحاكم الإنجليزية إذا كانت الجريمة لها علاقة بإنجلترا . وتتحقق تلك العلاقة لو وقعت تلك الجريمة على كمبيوتر متواجد في إنجلترا أو باستعمال كمبيوتر متواجد فيها أو مرورا بهذا الكمبيوتر[2].

ولتحديد مكان وقوع الجريمة يُرجع إلى القواعد العامة التي تميز بين الجريمة المؤقتة والجريمة المستمرة . فالجريمة المؤقتة تحدث زمنيا في لحظة معينة ومكانيا في المكان الذي وقع فيه ركن من أركانها . أما الجريمة المستمرة فإنها بسبب امتدادها في الزمن تعطي الاختصاص لكل مكان يتوافر فيه حالة الاستمرار كجريمة الاتجار بالمخدرات . ومقتضى الجريمة المستمرة أن الاختصاص ينعقد لكل محكمة تتوافر في دائرتها حالة الاستمرار . ومقتضى الجريمة المؤقتة أن الاختصاص ينعقد لمحكمة معينة ؛ هي تلك التي يقع النشاط أو النتيجة في

---

(١) انظر

Amanda Ryding, Management of Electronic Crime : Civil Aspects of Prevention and Containment, Journal of Financial Crime vol 6 N° 1 , August 1998, p. 56.

(٢) انظر

Amanda Ryding, management of Electronic Crime, id , p. 67

دائرة اختصاصها . أما الأثر الذي تخلفه الجريمة المؤقتة ، فإنه لا يعطي الاختصاص لمحكمة الدولة التي يشاهد فيها هذا الأثر ، مادام الأثر ليس من أركان الجريمة . والأمر على خلاف ذلك بالنسبة للجريمة المستمرة التي يشاهد فيها الجمهور الواقعة التي تشكل الجريمة في أكثر من دولة.

والمعول عليه في تحديد طبيعة الجريمة – وفقا لما تقضي به القواعد العامة – هو بطبيعة النشاط الإجرامي . فالسرقة جريمة وقتية ، بينما حيازة الأشياء المسروقة جريمة مستمرة . والنصب جريمة مؤقتة ، كما هو الحال بالنسبة لخيانة الأمانة، بينما الاتجار في الرقيق جريمة مستمرة .

وبناء عليه فإنه إذا قام المتعامل مع المجني عليه باستعمال رقم حساب هذا الأخير في سحب مبلغ مالي من بنك المجني عليه ، فإن الجريمة تقع في جزء منها في الدولة التي أصدر فيها المتهم الأمر بالسحب (لمبلغ أكبر من المتفق عليه) وجزء آخر من تلك الجريمة يقع في الدولة التي يتواجد فيها البنك المسحوب منه . ذلك أن الأمر يشكل جريمة خيانة أمانة والتي تتمثل

في سحب أكثر من المتفق عليه إخلالا بالأمانة التي تتمثل في تسلم مال على سبيل الأمانة وهو رقم الحساب . كما أن المبالغ التي تتواجد في حساب المجني عليه تشكل أمانة لدى المتهم الذي خُول بسحب جزء منها دون الجزء الباقي. ويقع ذلك على غرار من تسلم من المجني عليه مفتاح المخزن فيقوم بسحب بضاعة منه أكثر من المتفق عليه .

ولا نخال الأمر مختلفا بالنسبة لجريمة النصب التي تقع في مكان استعمال رقم الحساب (كوسيلة احتيالية) والمكان الذي يتواجد فيه البنك حيث يحدث التسليم . بيد أنه قد يحدث أن يعطي المتعامل مع صاحب الحساب

أمرا إلى هذا البنك بتحويل مبلغ نقدي زائد على المتفق عليه وذلك إلى دولة ثالثة أي دولة تختلف عن دولة المجني عليه ودولة المتهم . عندئذ يتحدد مكان وقوع الجريمة بثلاثة دول : دولة المتهم ودولة البنك المسحوب منه ودولة البنك المحول إليه. وبناء عليه يختص القضاء في هذه الدول الثلاثة بمحاكمة المتهم عن جريمة النصب.

تطبيقا لذلك قُضي بعدم اختصاص القضاء الإنجليزي بمحاكمة المتهم الذي كان يعمل في أحد البنوك في الكويت وقد قام قبل مغادرته الكويت للإقامة في إنجلترا بإعطاء أمر إلى كمبيوتر البنك الذي كان يعمل به هناك بتحويل مبالغ مالية من حسابات العملاء إلى حساب له فتحه في أحد البنوك في الكويت باسمه قبل سفره[1]. ويرجع ذلك إلى وقوع الجريمة في الكويت وعدم وقوع جزء منها على إقليم إنجلترا[2]. ويختلف الأمر عندما قام المتهم بإرسال خطاب من إنجلترا إلى البنك الكائن في الكويت والذي كان قد فتح فيه حسابا باسمه لتحويل المبالغ المالية من البنك الذي كان يعمل به .

فما قام به المتهم من إرسال خطاب إلى مدير البنك الثاني يطلب منه فيه تحويل المبالغ المالية التي وصلت إلى حسابه هناك إلى حساب له في إنجلترا تقع به جريمة السرقة وفقا لمفهوم القانون الإنجليزي لتلك الجريمة . هذه الجريمة تقع – وفقا للقانون الإنجليزي – على الحقوق things in action بمجرد وصول الادعاء بالحق وحتى قبل صرف هذه المبالغ [3] أي بمجرد وصول الخطاب من المتهم على ما سلف بيانه[4]. فوصول هذا الخطاب من

(1) J.C. Smith , The law of theft , seventh Edition, Butterworths , London , 1993, p.29.
(2) J.C. Smith , id .
(3) Chan Man- Sin v. A.G. of Hong Kong (1988) 1 All Er, 1, (1988) Crim. L R 319.

(٤) انظر سابقا رقم ٣٠ .

المتهم إلى مدير البنك الكائن في الكويت يمثل إدعاء بملكية هذه الأموال المحولة من البنك الأول، الأمر الذي تقع به جريمة السرقة بالمعنى المعرفة به في القانون الإنجليزي. ولما كان هذا الخطاب قد أرسل من إنجلترا إلى الكويت ، فإن القضاء الإنجليزي قد انتهى إلى وقوع جزء من جريمة السرقة على الإقليم الإنجليزي وبالتالي انتهى إلى اختصاص المحاكم الإنجليزية بنظر الدعوى(١).

وبناء عليه فإن إعطاء الأمر إلى كمبيوتر البنك في الكويت بتحويل مبلغ مالي - بدون وجه حق - من حسابات العملاء إلى حساب المتهم في إنجلترا يجعل المحاكم الإنجليزية مختصة بمحاكمة المتهم(٢).

- العبرة في تحديد مكان وقوع الجريمة هي بالأركان وليس بالأثر :

مؤدى ما سبق ذكره من أن المعول عليه في تحديد الاختصاص هو أركان الجريمة ومدى استمرارها في الزمن والمكان وليس الأثر الذي تخلفه أو مشاهدة الجمهور لذلك الأثر ، أن جريمة النصب وجريمة خيانة الأمانة لا تتحققان في جميع الدول التي يظهر فيها على شبكة الإنترنت رقم الحساب. فقيام أحد الأشخاص بمشاهدة هذا الرقم على تلك الشبكة لا يتحقق به ركن من أركان الجريمة . ومن ثمّ فإن الاختصاص بمحاكمة المتهمين بمثل هاتين الجريمتين لا ينعقد لمحاكم جميع الدول التي تظهر فيها شبكة الإنترنت.

وبناء عليه فإن قيام المتعامل مع صاحب الرصيد باستعمال رقم حساب هذا الأخير وسحبه مبلغا أكبر من المتفق عليه يشكل جريمة خيانة الأمانة. هذه الجريمة تقع في مكان إعطاء الأمر إلى البنك المسحوب عليه ، أي

---

(١) انظر سابقا رقم ١٣٥ .

(2) R. v. Thompson, (1984) 3 ALL. ER 565٧٩ (١٩٨٤)؛ Cr. App. Rep. 191 .

في دولة المتهم. يُضاف إلى ذلك أنها تقع في الدولة التي يتواجد فيها البنك المسحوب عليه والذي تلقى هذا الأمر ونفذه . وقد سبق القول بأن تسليم رقم الحساب إلى المتهم يعد بمثابة تسليم مفتاح لسحب كمية من البضاعة في مخزن معين. وبالتالي فإن مكان وجود هذا المخزن يتعلق بركن من أركان الجريمة ، وهو مكان وجود المال الذي أؤتمن عليه المتهم والذي خان الأمانة في خصوصه.

وفي الفرض الذي تقع فيه جريمة النصب من المشاهد لشبكة الإنترنت والذي يقوم باستعمال رقم حساب أحد الأشخاص المتعاملين عبر شبكة الإنترنت ، موهما كمبيوتر البنك بأنه مفوض من قبل صاحب الحساب في صرف مبلغ مالي من حساب هذا الأخير ، فإن الجريمة تقع في مكان إعطاء الأمر وكذلك في مكان وجود البنك . ذلك أنه من المقرر أن جريمة النصب تقع في مكان استعمال الوسيلة الاحتيالية وكذلك في مكان تسليم المال محل الجريمة . ومؤدى ذلك أن المتهم قد يأمر البنك المسحوب عليه بصرف مبلغ مالي في حساب يتواجد في أحد البنوك المتواجدة في بلد ثالث . فهناك إذن الدولة التي ينتمي إليها من قام بإصدار الإذن والتي تختلف عن دولة البنك المسحوب عليه . يُضاف إلى هاتين الدولتين دولة ثالثة وهي دولة البنك متلقي المبلغ المسحوب . ومؤدى ذلك أن الاختصاص بمحاكمة المتهم بجريمة النصب في هذه الحالة ينعقد للمحاكم في دول ثلاث . أما ظهور رقم الحساب عبر شبكة الإنترنت ، فما هو إلاّ الوسيلة التي مكّنت المتهم من ارتكاب الجريمة . وبالتالي لا ينعقد الاختصاص بمحاكمة المتهم في كل دولة من الدول التي تمر بها شبكة الإنترنت . أما قيام المتهم باستعمال الشبكة ذاتها في إصدار أمر إلى البنك المسحوب عليه ، أي في ارتكاب الجريمة، فإنه

لا يؤدى إلى القول بأن الاختصاص بالمحاكمة يصبح اختصاصا دوليا . فالعبرة هي إذن بأركان الجريمة وليس بالأداة التي استعملت في ارتكابها.

ومما يؤكد أن المعول عليه في تحديد الاختصاص بمحاكمة المتهم هو أركان الجريمة وليس الأثر الذي تخلفه أو الوسيلة التي استعملت في ارتكابها المثال الذي تقدمه لنا جريمة السب العلني وجريمة القذف . فأركان القذف تتمثل في الإسناد بطريق العلانية لواقعة تمس الشرف أو الاعتبار أو لواقعة لو صحت لاستوجبت عقاب المسند إليه . وبالمثل فإن الإسناد العلني يشكل ركنا في جريمة السب العلني، مادام محله كان صفة تستوجب احتقار الشخص لدى بني وطنه.

تلك العلانية مشروطة في الإسناد ، فهي ليست ركنا بذاتها ، ولكنها شكل يتطلبه القانون في ذلك الإسناد . فعندما يقوم المتهم بإسناد واقعة (في القذف) أو صفة (في السب) فإن مكان وقوع الجريمة يتحدد بمكان الإسناد. هذا المكان ليس إلا البلد التي كتب فيها المتهم الرسالة على الإنترنت. أما ظهورها على شبكة الإنترنت ، فإنه لا يعدو أن يكون أثرا من آثار الجريمة وليس ركنا فيها. ذلك أنه لا ينظر إلى العلانية بوصفها ركنا مستقلا ، ولكن بوصفها شرطا لفعل الإسناد نفسه. والقول بغير ذلك يؤدي إلى نتيجة غير منطقية ؛ وهي أن الجريمة تقوم من الناحية الزمنية وتستمر مادامت عبارات القذف أو السباب قائمة على شبكة الإنترنت. وهذا يجافي المنطق القانوني الصحيح. ذلك أن جريمة القذف وجريمة السب من الجرائم المؤقتة ولا تنتميان إلى الجرائم المستمرة . كما أن الفعل المعاقب عليه في هاتين الجريمتين هو الإسناد ، وقد تحقق الإسناد في لحظة زمنية معينة وبالتالي في مكان معين . ولا تعتبر شبكة الإنترنت مكانا لوقوع الجريمة ، وإنما وسيلة من وسائل

العلانية.

ويتماثل وضع علانية القذف والسب بطريق الإنترنت مع علانية هـذا القذف وذلك السب بطريق الصحف التي تُطبع في مكان معين ولكـن يـتم توزيعها في أقطار كثيرة . كما يحدث هذا التماثل مع حالة إذاعة ألفاظ القذف أو السب بطريـق القنـوات الفـضائية الـتي تعـبر حـدود الـدول ويـسمعها المشاهدون في بلدان عديدة. فالمشاهد في هذه الحالـة يـسمع الكلمـات الـتي تشكل الجريمة ، بل ويشاهد المتهم وهو يقوم بالفعل المعاقب عليه أي القذف في حق المجني عليـه أو توجيـه الـسب إليـه . هـذا الـسماع وتلـك المـشاهدة مكانهما غير مكان الإسناد . فهل تقع الجريمة في مكان الـسماع أو المـشاهدة أو أنها تقع في مكان الإسناد أي في المكان الذي يتكلم فيه المتهم ؟

هنا تبرز مرة أخرى أهمية تحديد مكان وقوع الجريمة والتمييز بينه وبـين المكان الذي يظهر فيه أثر من آثارها أو دليل من أدلتها . فمكان وقوع الجريمة هو المكان الذي يحدث فيه الركن المادي في الجريمة ، أي الإسناد .

وقد تُثار بقوة تلك المشكلة القانونية بالنـسبة للقـذف والـسب بطريـق الصحف والتي تُطبع في مكان معين ولكن تُوزع في عدة دول أي يُتاح للقراء في دول عديدة أن يقرءوا العبارات المؤثمة . نرى أن فعل الإسناد هو الـذي يشكل الركن المادي في جريمة القذف وفي جريمة السب ، وبالتالي فإن المعول عليه في وقوع الجريمة هـو مكـان وقـوع هـذا الفعـل وأن توزيـع الـصحيفة وظهورها في بلدان مختلفة ليس إلاّ أثرا من آثـار الجريمـة . وبالتـالي تختص محاكم الدولة التي حدث فيها فعـل الطبـع ولـيس فعـل التوزيـع . ويـصبح مفهوما عندئذ أنه إذا أُعيد طبع الصحيفة في بلد آخر غير البلدان التي وزعت فيها ، فإن المعول عليه في تحديد مكان وقوع الجريمة هو فعل الطبع ، لأنه هو

الذي يشكل فعل الإسناد بطريق العلانية . يستوي بعدئذ أن تحدث العلانية في بلد واحد أو في بلدان عديدة.

ولا شك أن تحديد وقوع الجريمة من ناحية المكان يتعلق بتحديد وقوعها من ناحية الزمن. فمادامت الجريمة تحدث زمنيا عند أول توزيع للصحيفة ، فإنه لا عبرة عندئذ بما يحدث من وقائع توزيع أخرى لنفس الصحيفة التي احتوت العبارات المؤثمة . وبالتالي يتحدد زمن وقوع الجريمة وكذلك مكان وقوع الجريمة في تلك اللحظة ، دون عبرة بما يستتبع ذلك من وقائع.

وقد أحسن القضاء الكويتي عندما قضى بوقوع الجريمة عند أول صدور للصحيفة التي حملت الألفاظ المعاقب عليه بوصف السب العلني أو بوصف القذف، حتى ولو أُعيد طبع الصحيفة الأسبوعية مرة أخرى عند نفاذ الطبعة الأولى[١]. ومؤدى ذلك أن الجريمة تتم من الناحية الزمنية عند أول طبع للصحيفة.

وكذلك فإن سماع ألفاظ السباب أو القذف أو مشاهدة المتهم وهو يقوم بفعل الإسناد أثر من آثار الجريمة ودليل من أدلتها . وبناء عليه فإن الاختصاص ينعقد للمحكمة التي وقع في دائرتها فعل الإسناد ، وليس في كل مكان سمع فيه المشاهد الكلمات المشكلة للجريمة عبر القناة الفضائية التي تبث في بلدان العالم المختلفة . وبالمثل فإن جريمة القذف وجريمة السب العلني لا تقعان بطريق الإنترنت في جميع بلدان العالم التي تغطيها تلك الشبكة والتي يُتاح فيها لكل فرد قراءة العبارات التي كانت محلا للإسناد.

---

(١) محكمة الاستئناف الكويتية ، جلسة ٢٦ / ١٠/ ١٩٩٧ ، رقم ١٤٤٢/٩٧ ج م - ٦١/ ٩٦ جنح صحافة

المطلب الرابع

صعوبة تحديد المسئول جنائيا

- أسباب تلك الصعوبة:

يرتبط بالطبيعة الخاصة لشبكة الإنترنت صعوبات قانونية تتعلق بتحديد المسئول جنائيا عن الجرائم التي تقع عن طريق هذه الشبكة . فقد تقع جرائم باستعمال تلك الشبكة مثل جرائم النصب وخيانة الأمانة. وقد تقع جرائم تستغرق بعض الوقت مثل عقد مؤتمر صحفي بين المشاركين فيه عن طريق الشبكة تتخلل الحديث خلال هذا المؤتمر عبارات تشكل سبا أو قذفا أو جريمة من جرائم أمن الدولة أو من جرائم الإخلال بالحياء العام أو غير ذلك من جرائم.

وترجع الصعوبة في تحديد المسئول جنائيا إلى أن مستعمل شبكة الإنترنت قد يصعب تحديد مكانه ، في داخل البلاد أو في خارجها . ومن هنا كان التهرب من إجراءات الدعوى الجنائية أمرا ميسورا . ومن هنا أيضا كان ضروريا وضع تنظيم قانوني للمسئولية الجنائية للأشخاص الذين لهم دور في استعمال أو استغلال شبكة الإنترنت.

- مسئولية المستعملون والمستغلون لشبكة الإنترنت:

الأصل أن المسئول جنائيا هو مستعمل شبكة الإنترنت الذي ارتكب جريمة معينة عن طريق تلك الشبكة. بيد أنه قد يصعب تحديد هوية هذا المستعمل. وقد يجد المحقق صعوبة كبيرة في اقتفاء أثر هذا المستعمل ، إذ قد يعمد إلى إخفاء هذا الأثر ، عندما يستخدم جهازا متواجدا في مكان عام ويقوم بإدخال بيانات أو رسائل يعاقب عليها القانون . على خلاف ذلك

فإن المستعمل يمكن معرفة مكانه من واقع اسم المستخدم user name وكلمة السر password التي من خلالها يتعامل مع شبكة الإنترنت . هذه البيانات من شأنها أن تساعد في تحدد مكان الجهاز الذي قام المستعمل بإرسال الرسالة منه . وقد يعمد المستعمل إلى وسائل فنية بغرض إزالة ما يمكن أن يساعد على معرفة هوية الجهاز الذي يبث منه الرسائل المؤثمة أو قد يستعمل جهازا متواجدا في مكان عام كالمطارات مثلا . يضاف إلى ذلك أن المستعمل قد يتواجد في الخارج ، وتثور صعوبة قانونية بخصوص محاكمته عن الجريمة التي ارتكبها.

هذه الصعوبات القانونية تثور بالنسبة للمستعمل ، سواء لجأ إلى إرسال رسائل إلى البريد الإلكتروني ، أو لجأ إلى إرسال رسائل مفتوحة على شبكة الإنترنت أو استعمل صفحة خاصة به على أحد المواقع site.

- الأهمية القانونية لمقدم خدمات الإنترنت:

لما كان من الميسور معرفة الشخص الذي يقوم على تقديم خدمات الإنترنت، بما في ذلك إتاحة الفرصة لعقد مؤتمر صحفي بطريق الإنترنت أو بث صفحة خاصة بالمشترك ، فإنه كان من الضروري تنظيم المسئولية الجنائية لمقدم تلك الخدمات provider ، وكذلك للشركة التي تنتج برامج يقوم مقدم الخدمات ببثها. ولا ننسى أنه قد يكون هناك أشخاص فنيون يقومون بإعداد تلك الخدمات ، ومنها تنسيق تلك الصفحة من الناحية الفنية تمهيدا لبثها.

ويثير اختيار النظام القانوني الذي يُطبق على مقدم خدمات الإنترنت مشكلة قانونية : هل يسري عليه النظام القانوني لرئيس التحرير في جريدة أم

أنه من الأنسب أن يتدخل المشرع ليورد نظاما قانونيا خاصا يناسب وضعه القانوني الخاص والمختلف عن رئيس تحرير الجريدة ؟

أثير هذا التساؤل أمام القضاء الفرنسي واختار تطبيق النظام القانوني لرئيس تحرير الجريدة على مقدم خدمات الإنترنت[1]. وكان يحدو القضاء في ذلك الحرص على الاّ يفلت مقدم الخدمات من المسئولية وقد أفلت المستعمل الذي بثّ الرسائل المعاقب عليها ، وذلك بسبب عدم معرفته . ولم يكن غائبا عن نظر محكمة النقض الفرنسية أن مقدم الخدمات يجب الاّ يدرأ مسئوليته في متابعة مؤتمر صحفي عُقد على شبكة الإنترنت (في هذه القضية) وتخللته عبارات يعاقب عليها القانون، ولم يقم مقدم خدمات الشبكة بقطع الإرسال عنها . كما كان ماثلا تحت نظر المحكمة أن مقدم خدمات الإنترنت يقع عليه التزام ببذل العناية اللازمة لمعرفة الأشخاص الذين يشتركون في البث على شبكة الإنترنت عن طريق المدخل الذي يقدمه لهم. والحكمة في ذلك تدرك حقيقة أن ما يجنيه مقدم الخدمات من أرباح تبرر ما يمكن أن يتكبده من نفقات لمتابعة ما يتم بثه عن طريق المنفذ الذي يقدمه.

ومع ذلك فإن تشبيه مقدم خدمات الإنترنت برئيس تحرير الجريدة أمر ليس محلا للإجماع ، ذلك أن المقالة في الجريدة ثابتة في محتواها الذي يقرأه أو يتعين عليه أن يقرأه رئيس التحرير . أما ما يتفوه به المؤتمرون على شبكة الإنترنت من أقوال مؤثمة ، فهو أمر يصعب التنبؤ به . ومع ذلك فإن من واجب مقدم خدمات الإنترنت أن يتدخل بقطع البث عن طريق منفذه.

هذا الواجب المتمثل في المتابعة يستدعي أن يورد المشرع من التنظيم

(1) Crim. 8 déc. 1998, Bull. crim. n° 335; Jacques FRANCILLON , " Infractions relevant du droit de l'information et de la communication" , Rev. sc. Crim. 1999, chr. 606.

القانوني ما يكفل تجريم الإهمال الذي ينسب إليه. كما أن ذلك التجريم لا يستبعد تأثيم سلوك هذا الشخص إذا تمّ بشكل عمدي. وعلى هذا فإن من المناسب إيراد نوعين من الجرائم التي يمكن أن تنسب إلى مقدم خدمات الإنترنت: النوع الأول عمدي والثاني غير عمدي. وهذا يبرهن على حقيقة أن مقدم خدمات الإنترنت يختلف في وضعه القانوني عن رئيس تحرير الجريدة ، الأمر الذي يستدعي تنظيما قانونيا متميزا.

خاتمة ونتائج البحث

تناول هذا البحث موضوعا متجددا متناميا يتعلق بجرائم تقنية المعلومات وخاصة في جوانبه الإجرائية التي لا تزال جديدة في داخل موضوع هو أصلا متجدد بقدر ما تتجدد وتتطور تكنولوجيا المعلومات التي لا تكف عما هو جديد في كل عام.

وقد أبرز البحث ما للإجراءات الجنائية في مجال جرائم تقنية المعلومات من جوانب تختلف فيها عن الإجراءات الجنائية في غيرها من ائم سواء في مرحلة جمع الاستدلال أو في مرحلة التحقيق الابتدائي أو خيرا في مرحلة المحاكمة.

وقد انتهى البحث إلى نتائج من أهمها ما يلي:

- ضرورة أن ينظم المشرع الجوانب الإجرائية المختلفة عند مكافحته جرائم تقنية المعلومات والاّ يكتفي بوضع قواعد موضوعية خاصة بالتجريم والعقاب فقط كما فعل المشرع الاتحادي في الإمارات الذي اقتصر في القانون رقم ٢ لسنة ٢٠٠٦ على إيراد نصوص خاصة بالتجريم والعقاب فقط ولم يتناول الجوابب الإجرائية لتلك الجرائم على أهميتها.
- ضرورة إيجاد وحدات متخصصة من رجال الضبط القضائي ومن المحققين وكذلك دوائر من المحاكم تتخصص في محاكمة المتهمين بهذا النوع من الجرائم.
- ضرورة تنظيم واجب التعاون بين رجال الضبط القضائي والجهات العامة والجهات الخاصة التي تمتلك أجهزة معالجة المعلومات والتي

يمكن أن تحوز معلومات تفيد في كشف الحقيقة عن وقوع جريمة معينة أو نسبتها إلى فاعلها، وذلك من ناحية شروطه وأحواله، مع التحفظ الخاص بالملتزمين بسر المهنة.

- من الضروري أن يقوم المشرع بتنظيم الإجراءات الجنائية فيما يتعلق باعتراض وتسجيل المراسلات الإلكترونية وذلك نظرا لاختلافها عن الاتصالات الهاتفية وكذلك عن المراسلات البريدية.
- ضرورة النص على الحل المتبع عندما يكون الجهاز المراد تفتيشه مرتبطا بغيره من الأجهزة داخل شبكة واحدة.
- من المناسب النص على مدى حق رب العمل ومدى حق المدير الإداري في تفتيش الأجهزة الخاصة بالعمل ومدى حقهما في مراقبة تلك الأجهزة وحدود هذا الحق إن وجد.
- من المفيد تنظيم إجراءات الضبط الخاصة بالمعلومات وذلك لعدم كفاية إجراءات الضبط التقليدية والتي ترد على أشياء محسوسة.
- من المتعين أن يحل القانون مسألة اختصاص سلطة التحقيق واختصاص المحكمة فيما يتعلق بمحاكمة المتهمين بجرائم تقنية المعلومات.
- ضرورة النص على حجية المستندات الإلكترونية سواء في المواد الجنائية أو في المواد المدنية مع تحديد الشروط اللازمة للاعتداد بتلك المستندات وتنظيم الموضوع عندما يكون هناك تعارض بين المستندات الإلكترونية والمحررات المكتوبة.

الباب الثالث

الاحتيال باستعمال شبكة الإنترنت

موضوع الدراسة:

تتناول هذه الدراسة علاقة الاحتيال بالجريمة المنظمة لكى يكشف أبعاد هذا النشاط الإجرامى اذا كانت عصبة إجرامية تقوم به بصفتة نشاطاً وحيدا لها أو بصفتها نشاط من أنشطتها الأساسية.

ويرتبط ببيان هذة العلاقه ما يتسم به نشاط الاحتيال من جانب تلك العصابات من طابع عبر الدول وخاصة عندما يتم استخدام شبكة الانترنت للايقاع بضحايا تلك العصابات التى تستولى على أموالهم بطريقة من طرق الوسائل الاحتيالية. ولا شك أن هذا الطابع عبر الدول من شأنة أن يخلق مشكلات قانونية منها ما يتعلق بازدواجية التجريم وعدم جواز المحاكمه عن فعل واحد مرتين، ومنها ما يتعلق بالاختصاص بالتحقيق والمحاكمة فى هذا النوع من الجرائم ومنها ما يتعلق بالتعاون الدولى.

إشكاليات الدراسة:

يثير هذا الموضوع عدة إشكاليات قانونية يرمى إلى دراستها وإبداء الرأي فيها. من هذة الإشكاليات ما يلى: ما هى شروط وأركان جريمة الإحتيال المنظم؟ هل يختلف الاحتيال المنظم عن احتيال غير المنظم؟ ما هى المشكلات القانونية التى يثيرها تجريم الإحتيال المنظم؟ ما هى المخاطر والمحازير التى يثيرها بالنسبة للحقوق الأساسية ومنها حقوق الإنسان؟ هل من المقبول أن نخرج عن القواعد العامة فى قانون العقوبات (الخروج على بعض مظاهر مبدأ شخصية المسئولية مثلاً) وقانون الإجراءات الجنائية بأن ندرج الإحتيال ضمن الجريمة المنظمة (الخروج على قواعد الإختصاص مثلا)؟ ما هى جهة التحقيق والمحاكمة المختصة بمحاكمة الإحتيال عبر الحدود عند إرتكاب الجريمة باستخدام شبكة الإنترنت خاصة؟

ظهور المشكلة وأهميتها؟

ظهرت فى الآونة الأخيره عصابات تتجه الى الإحتيال على الغير مستغلة فى ذلك شبكة الإنترنت فى الإحتيال على ضحاياها من بلدان بعيده فيصعب بالتالى القبض عليهم ومحاكمتهم. ومن هنا كانت أهمية دراسة مدى دخول الاحتيال كنشاط من أنشطة الجريمة المنظمة جنباً إلى جنب مع تجارة المخدرات والإتجار بالبشر....

وترجع بعض أسباب المشكلة إلى أن التشريعات تعتبر الاحتيال من الجنح أى أنها لا تنظر إلية بعين الخطورة، كما ترجع بعض تلك الأسباب إلى عدم توافر الطرق الإحتيالية فى كثير من الحالات حيث يقوم المحتال بالإتصال بالمجنى علية مبلغاً إياه بأنة كسب ثروة معينة من ميراث بسبب وفاة قريب له أو من كسبه جائزة معينة وأن المطلوب منه هو دفع مصاريف الحصول على هذا الميراث أو تلك الجائزه لكى يقوم بقبض مبلغها، ويتضح أنه أمر كاذب وأنه ليس إلا وسيلة للإستيلاء على أموال الغير. غير أنه فى بعض الحالات يستعين المتهم بأوراق رسمية مزورة تفيد وفاة أحد الأقارب وأن له تركة فى بلد معين وبأن شخاصاً معيناً يقيم فى بلد آخر هو وريث له وأن من حقة الحصول على نصيبه فى هذا الميراث. فى هذة الحالة يتوافر فى الفعل الطريقة الإحتيالية فى القوانين الموضعية. مع ملاحظة أن الشريعة الإسلامية لا تستلزم فى الإحتيال ولكن يكفى فيه مجرد الكذب والإستيلاء على أموال الناس بالباطل.

خطة الدراسة:

تدور خطة الدراسة على تقسيمه إلى مبحثين:

المبحث الأول: ويعالج الاحتيال بوصفه نشاطاً من أنشطة الجريمة المنظمة

المبحث الثانى: ويعالج المشكلات القانونية المتعلقة بالاحتيال المنظم

الفصل الأول

الاحتيال بوصفه نشاطاً من انشطة

الجريمة المنظمة

التعريف بالجريمة المنظمة وموضوع الاحتيال منها :

الجريمة المنظمة بين الظهور والانحسار:

بذلت محاولات عديدة من كتاب ولجان لتعريف الجريمة المنظمة وذلك بتحديد خصائصها التى تتميز بها عن غيرها من الجرائم ، منها عنصر التنظيم، وعنصر الاستمرار فى الزمان[1] وعنصر خطورة الجرائم التى ترتكبها ، وعنصر العنف أو التهديد بة .

من أهم تلك التعريفات ما أوردتة إتفاقية الأمم المتحدة لمكافحة الجريمه المنظمه سنة ٢٠٠٣ حيث تعرف المادة الثانيه منها تلك الجريمه بقولها "جماعة إجرامية منظمة" جماعة ذات هيكل تنظيمى ، مؤلفة من ثلاثة أشخاص أو أكثر ، موجودة لفترة من الزمن وتعمل بصورة متضافره بهدف إرتكاب واحدة أو أكثر من الجرائم الخطيره أو الأفعال المجرمة وفقاً لهذة الإتفاقيه، من أجل الحصول ، بشكل مباشر أو غير مباشر ، على منفعة ماليه أو منفعة ماديه أخرى ".

أما التشريعات المقارنة فإن كثيراً منها لا يعرف هذا التجريم ولكن يكتفى بإعتبار ذلك من قبيل الظروف المشددة فى جرائم معينه ، منها التشريع الألمانى والتشريع المصرى والأنظمة المعمول بها فى المملكة العربية السعوديه. من ذلك أن عقوبة غسل الأموال تشدد فى المملكة العربية السعوديه إذا وقعت الجريمة من خلال عصابة منظمه (المادة السابعة عشر من

---

(١) د. عبداللة سيف عبدالله الشامسى ، الجريمة المنظمة ، رسالة ، جامعة القاهرة ، ٢٠٠٣ .

المرسوم الملكى بتاريخ ٢٥/٦/ ١٤٢٤).

ومع ذلك فإن هناك من التشريعات ما يعرف هذا التجريم فى شكل جماعة البغاه association de malfaiteurs الذى يعرفة القانون الفرنسي والكندى، وتجريم مشابه وإن كان مختلفاً فى القانون الأمريكى تحت مسمى conspiracy . كما تصدى المشرع الأمريكى لتعريف الجريمة المنظمة فى صدد بعض الجرائم كالقانون المسمى بـ[1] law ٩٠ -٣٥١ , ١٩٦٨the omnibus crime control and state streets act of والذى عرف الجريمة المنظمة بأنها " أنشطة غير مشروعة لأعضاء فى رابطة منظمه بشكل كبير تتورط فى تقديم بضائع وخدمات غير مشروعه منها لعب القمار، الدعارة، القروض الربوية، المخدرات، التهديد والابتزاز وأنشطة أخرى غير مشروعة[2][3].

- يبقى أن هذا التجريم ينتشر مع الوقت وان كانت المحكمة الدستوريه فى مصر قد قضت بعدم دستورية الماده (٤٨) من قانون العقوبات فى مصر والتى كانت تعاقب على الاتفاق الجنائى[4] ، واضعة بذلك

(1) Sabrina Adamoli, Andrea Di Nicola, Ernesto U.Savona and Paola Zoffi, European Institue for Crime Privention and Control, affiliated with the United Nation (HEUNI)
P.O.Box 161,FIN-00131 Helsinki, finland, Publication Series No.31, ORGANISED
CRIME ARAUND THE WORLED Helsinki 1998

(2) Organised ceime means the unlawful activites Of members of a highly organized, disciplinded association engaged in supplying illegal goods and services, including but not limited to gambling ,prostitution ,loan sharking, narcotics, labour racketeering,and other unlawful activities "

(3) Michael D. Lyman, GVary w. potter, Organized crime, prentice – Hall Company, Inc ١٩٩٧,p. ١٨٣(٤) bribry of judicial officers; bribery of officials; frauds upon the gov Morles; keeping a gaming or betting house; betting, pool – selling; bookmaking ; keeping

(٤) حكم المحكمة الدستورية بتاريخ ٢ يوليو سنة ٢٠٠١، قضية دستورية عليا رقم٢١ ق بتاريخ ٢٢ يونيو سنة ١٩٩٩

- د. محمد سامى الشوا ، الجريمة المنظمة دار النهضة العربية ' ١٩٩٨ ، ص ٣٩

عقبة نحو تبنى المشرع المصرى هذا الاتجاة الذى بدأ يتعاظم فى التشريعات المقارنه فى الآونة الأخيره. فقد كانت المادة ٤٨ عقوبات مصرى تنص على أنه " يوجد إتفاق جنائى كلما إتحد شخصان أو أكثر على إرتكاب جناية أو جنحة ما أو على الأعمال المجهزة أو المسهلة لارتكابها . ويعتبر الاتفاق جنائياً سواء أكان الغرض منه جائزاً أم لا إذا كان إرتكاب الجنايات أو الجنح من الوسائل التى لوحظت فى الوصول إلية . ..." ومع ذلك فإن هذا الحكم لا يحول دون إيجاد تجريم للجريمة المنظمة بشرط احترام المبادئ القانونية للقانون الجنائى .

مدى انتماء الاحتيال إلى الجريمة المنظمة :

على الرغم من أن الاجرام المنظم يسعى الى الربح غالباً من وراء الأنشطة الاجرامية التى يمارسها كالإتجار فى المخدرات أو غسل الأموال [١] وعلى الرغم من أن الإحتيال يسعى هو الآخر الى تحقيق الربح، إلا أن ثمة صعوبة فى القول بأن الاحتيال أو النصب من الأنشطة الأساسية للجرائم المنظمة، ويرجع ذلك إلى التالى:

أولاً : الجريمة المنظمة تعتمد على استعمال العنف أو التهديد به، من ضمن العناصر المميزة للتنظيم ، بينما لا يتناقر الاحتيال بطبيعته مع العنف.

ثانياً : يعتمد الاحتيال على القيام بعمليات غالبيتها ذات طابع فردى، فالاحتيال لا يحتاج الى عنصر التنظيم العصابى .

ثالثاً : يعتمد المحتال على الاستيلاء على أموال الغير ثم الاختفاء عن أعين

---

(١) د. محمد سامي الشوا، الجريمة المنظمة ، دار النهضة العربية، ١٩٩٨ ص ٣٩

رجال الضبط القضائي حتى لا يتم الإمساك به، والأمر على خلاف ذلك بالنسبة للجريمة المنظمة التي تعتمد على عنصر الاستمرار.

ومع ذلك فإن هناك من التشكيلات العصابية ما يقوم بنشاط الاحتيال بصفة أساسية متخصصاً في هذا النشاط ، كالشركات التي تحتال على العمال بدعوى إلحاقهم بالعمل بالخارج أو تلك التي تستولى على أموال الغير بدعوى توفير أعضاء بشرية يحتاجون اليها كما في حالة زرع كبد أو كلية في الصين مثلاً ، ولذا يجب أن نميز بين الفروض التالية:

الفرض الأول : وفيه يكون الغرض من التنظيم الإجرامي أن يقوم بنشاط الاحتيال أي يكون هذا النشاط هو الرئيسي في سبيله لتجميع الأموال كما في الأمثلة السابقة.

الفرض الثاني : أن يقوم التشكيل العصابي بنشاط إجرامي معين كالإتجار في المواد النووية ، ويقوم بشكل عرضي أحياناً بالاحتيال كما لو أوهم أخرين بأن المواد ذات طبيعة نووية .

على خلاف تلك الرؤية التي تدخل نشاط الاحتيال ضمن نشاط الجريمة المنظمة ، فإنة من الأفضل والواقعي أن يورد القانون ظرفاً مشدداً لعقوبة الاحتيال إذا اصدر من عصبة منظمة. بيد أنه يلاحظ أن المشرع الفرنسي قد ألغي ما قد أوردة من إعتبار العصبة الإجرامية ظرفاً مشدداً في جريمة الاحتيال secroquerie)) بمقتضى القانون رقم ٢٠٤ لسنة ٢٠٠٤ والصادر في ٩ مارس سنة ٢٠٠٤ (مادة٦-x) ، مكتفياً باعتبار إرتكاب بعض الجرائم من عصبة إجرامية bande organisee ظرفاً مشدداً كما هو الحال في جريمة غسل الأموال (مادة ٣٢٤-١ عقوبات فرنسي). أما

القانون المصرى فإنه لم يعرف ارتكاب جريمة من جرائم الأموال أو من جرائم الأشخاص من جانب عصبة كظرف من الظروف المشددة للعقوبة ذلك أن ظرف التعدد فى السرقة مثلاً يختلف عن إرتكاب السرقة من جانب عصبة منظمة وهو ما لم يتبناه المشرع المصرى فى مواد السرقة. ومع ذلك فإن المشرع المصرى يجرم فى بعض جرائم أمن الدولة تكوين عصبة إجرامية الغرض منه الدعوة بأية وسيله إلى تعطيل أحكام الدستور أو القوانين أو منع إحدى مؤسسات الدولة أو إحدى السلطات العامة من ممارسة أعمالها أو الإعتداء على الحرية الشخصية للمواطن أو غيرها من الحريات والحقوق العامة التى كفلها الدستور والقانون أو الإضرار بالوحدة الوطنية أو السلام الإجتماعى (مادة ٨٦ مكرر عقوبات مصرى.

المساهمة فى الإحتيال المنظم:

فى حالة قيام تنظيم عصابى بارتكاب جريمة الاحتيال ضمن أنشطته، كالعصابات التى يوهم المجنى عليهم فى دول أخرى بأن لهم أموالاً قد ورثوها مثلاً عن قريب لهم فيها وأستعانوا بالغير فى إيهام هؤلاء المجنى عليهم ، فإن الجريمة تقع فى أكثر من شخص وتثار مشكلة قانونية تتعلق بمدى مساءلتهم جنائياً عن تلك الجريمة ومدى مسئولية أعضاء العصابة عن تلك الجريمة .

يتعين بادئ ذى بدء القول أن جريمة الاحتيال من الجرائم العمدية التى يلزم لتوافرها قيام العلم والإرادة لدى الفاعل والشريك أى أن يعلم باقى أعضاء التنظيم بأن هناك نشاطاً يتمثل فى الاحتيال على المجنى عليهم. كما أن جريمة الاحتيال شأنها فى ذلك شأن غيرها من الجرائم لا تقوم إلا إذا توافر الركن المادى لها والذى يتمثل فى الاستيلاء على أموال الغير بالاستعانة بوسائل احتيالية. ومؤدى ذلك أن يقوم الفاعل أو الشريك بجزء

من النشاط والذى يتمثل فى ممارسة الاحتيال أو الاستيلاء على المال. والأمر على خلاف ذلك بالنسبة للجريمة المنظمة.

لذلك نرى أن الركن المادى فى الجريمة المنظمة يختلف عن الركن المادى فى الجريمة العادية أى أن وقوع الاحتيال ممن ينتظمون فى مشروع إجرامى منظم للقيام بالاحتيال يختلف عمن يقومون بالاحتيال فى شكل فردى أو حتى جماعى دون أن يندرج فى شكل تنظيم إجرامى. ويرجع السبب فى ذلك إلى طبيعة الجريمة المنظمة التى تقتضى المسئولية التضامنية.

فما يميز الجريمة المنظمة عن الجريمة غير المنظمة هو أن هناك توزيعاً للأدوار بين أعضاء العصبة الاجرامية التى إتفقت إرادتها على تكوين تجمع منظم من الناس للقيام بمشروع إجرامى مستمر فى الزمان هدفه ارتكاب جريمة أو جرائم معينة، أى أن الركن المعنوى القائم على العلوم والإرادة ؛ إرادة الاشتراك فى الجماعة الاجرامية هو الذى يشكل الأساس القانونى الذى تستند إليه المسئولية التضامنية من الناحية الجنائية ، وليس المسئولية الفردية . ومؤدى ذلك أن كل عضو من أعضاء الجماعة الإجرامية لا يسأل فقط عن فعله الذى قام به أو ساهم فيه ولكن يسأل أيضاً عما يقوم به الأعضاء الأخرون.

توزيع الأدوار وأثرة على المسئولية الجنائية للأعضاء فى جرائم المخدرات:

مما يؤكد أن اتفاق إرادات أعضاء العصبة الإجراميه على إرتكاب جريمة أو جرائم معينة يؤدى إلى التضامن فى المسئولية ما طبقته أحكام القضاء فى بلدان عديدة فى خصوص استيراد وجلب المخدرات من تجمع من الأفراد اتفقت إرادتهم على هذا الجلب حيث يعتبرون فاعلين أصليين فى عملية الإستيراد أو الجلب بغض النظر عن دور كل منهم فى تلك العملية[1] .

وقد عبرت محكمة التمييز الكويتية عن تلك الفكرة بشكل صريح

---

(١) د. فيصل عبدالله الكندرى ، غنام محمد غنام ، شرح قانون الجزاء الكويتى ، القسم الخاص الطبعة الأولى ، ٢٠٠٦ ص ٥٦٥

بقولها " عملية الاستيراد بحسب خطة تنفيذها تنطوى على عدة أفعال وكل من يتدخل فى تنفيذ أى فعل من هذه الأفعال يعتبر مرتكباً لفعل الاستيراد سواء صدر منه الفعل التنفيذى أو من ساهم فيه بالنقل أو من يتم النقل لحسابه أو مصلحته ولو لم يصدر منه شخصياً فعل النقل أو المساهمة فيه ، وذلك متى كان الفعل يمثل حلقة من حلقات عملية الإستيراد على نحو يكفل إستيراد المخدرات "[1].

وقد سبق لمحكمة النقض المصرية أن عكست تلك الفكرة فى أحكامها فى جرائم جلب المخدرات بقولها إن " الجريمة إذا ارتكبت من عدة أفعال سواء بحسب طبيعتها أو طبقاً لخطة تنفيذها فإن كل من تدخل فى هذا التنفيذ بقدر ما يعد فاعلاً مع غيرة ، ولو أن الجريمة لم تتم بفعلة واحدة ، بل تمت بفعل واحد ممن تدخلوا معه فيها، إذا وجدت لدى الجانى نية التدخل تحقيقاً لغرض مشترك هو الغاية النهائية من الجريمة بحيث يكون كل منهم قد قصد قصد الفاعل معه فى إيقاع تلك الجريمة وأسهم فعلاً بدور فى تنفيذها "[2] ، وقد أكدت المحكمة فى تلك القضية على أن " المتهمين الثلاثة إتفقت كلمتهم على جلب المواد المخدرة وأن كل منهم أسهم- حقيقاً لذلك- بالدور الذى أعد له فى خطة تنفيذ تلك العملية.

تطلب الركن المادى لقيام المسئولية التضامنية عن الإحتيال المنظم :

على الرغم من المسئولية التضامنية التى من المنطقى أن تسرى على أعضاء العصبة الإجرامية الواحدة ، فإنه من الضرورى أن ينسب إلى عضو

---

(١) تمييز كويتى ١٩/٢/١٩٩٠ طعن رقم ٣١٤/٨٩ جزائى ، مجموعة القواعد القانونية فى المواد الجزائية ، يونيو ١٩٩٦ ص ٦٧٦

(٢) نقض ١١ فبراير سنة ١٩٧٤ ، مجموعة أحكام النقض س ٢٥ رقم ٢٩ ص ١٢٦

العصبه عملاً مادياً وذلك إحتراماً لمبدأ المسئولية الجنائية الشخصية

ومبدأ قرينة البراءة التى يقتضى كل منها عدم الإكتفاء بالركن المعنوى فى الجريمة دون الركن المادى؛ فلا يسأل شخص عن مجرد نواياه وبالتالى فإن المسئولية الجنائية لا يمكن أن تستند إلى توافر القصد الجنائى دون إرتكابة لفعل مادى.

غير أن التفرقة بين الفعل المادى الذى يشكل الجريمة فى حالة قيام العصبة الإجراميةبالاحتيال يختلف عن حالة إرتكاب الجريمة بطريقة فردية أو حتى فى حالة تعدد المساهمين دون توافر العصبة الإجرامية. ففى حالة العصبة الإجرامية يكفى أن يقوم العضو بأى فعل يتجه مع أفعال غيره من أعضاء العصابة إلى وقوع جريمة الإحتيال مثلاً. فمن يقوم بتزوير مستندات وهو عضو فى العصابة لكى يقوم غيره من أعضائها باستخدامها فى النصب على المجنى عليهم يسأل عن جريمة النصب ، بوصفه فاعلاً فى جريمة الإحتيال المنظم وليس بوصفه شريكاً. فالمسئولية الجنائية عن جريمة النصب على الرغم من أنه لم يقم بنشاط الإحتيال عن المجنى علية ، ذلك لأن فعله ينضم إلى أفعال غيرة من أعضاء العصابة فى تشكيل الإحتيال المعاقب علية، بل إن فعل تزوير المستندات التى قام بها هذا العضو عن علم أنها سوف تستخدم فى ارتكاب النصب وتم استخدامها بالفعل يجعل منه فاعلاً وليس شريكاً فى الجريمة. وهذا ما تتميز به المسئولية الجنائية فى حالة الجريمة المنظمة عن الجريمة المعتادة. والأمر كذلك بالنسبة لعضو العصابة الذى يحصل على عناوين المجنى عليهم لكى يتم الإحتيال عليهم من جانب شركاء له فى العصابة.

خصائص الإحتيال المنظم:

يتميز الإحتيال المنظم عن الإحتيال كمشروع فردى أو حتى الاحتيال مع تعدد المساهمين بالخصائص التالية:

(أ) الإستمرارية:

تتميز الجريمة المنظمة بعنصر الاستمرار[1]. وإذا تعلق الأمر بالإحتيال، فإنه يقصد بالاستمرارية فى الاحتيال ما يقع من تنظيم إجرامى له طابع الاستمرار فى الزمان وليس وليد عملية لحظية تقع وتنتهى. ويترتب على ذلك نتيجتان قانونيتان:

أولهما: أن الاحتيال المنظم له طابع الاستمرار فى الزمان

ثانيهما: أن الاحتيال المنظم له طابع الاستمرار فى المكان

إذا قرر المشرع الانضمام الى عصبة إجرامية يكون من ضمن أغراضها إرتكاب فعل من أفعال الاحتيال ضمن أنشطة إجرامية أخرى، فإن تلك الجريمة تكون منتمية إلى الجرائم المستمرة . هذا الاستمرار يكون فى الزمان كما هو فى المكان.

ويتريب على الاستمرار فى الزمان أن مدة التقادم لا تبدأ ما دام أن تلك العصبة لا تزال قائمة وتمارس نشاطها. ويترتب على الاستمرار فى المكان نتائج قانونية تتعلق بالاختصاص بالتحقيق وبمحاكمة المتهمين فى تلك الجريمة، فيؤول الاختصاص بالتحقيق والمحاكمة إلى مكان وجود التنظيم

(1) Christine VAN DEN WYNGAERT, les transformations du droit international pénal en réponse au défi de criminalité organisée, rapport présenté colloque préparatoire sur " Les sysémes pénaux á l'épreuve du crime organize, Ultrecht (Pays-Bas) ,13-16 mai 1998 , p.58

الاجرامى ولا يلزم أن يكون هذا التنظيم قد مارس الاحتيال فى نفس مكان وجود التنظيم، ذلك أن جريمة الانضمام إلى تشكيل عصابى لا يلزم لتوافرها أن يقوم أعضاؤها بالاحتيال فى نفس مكان وجود التنظيم ، بل تقع الجريمة لو وقعت أفعال الاحتيال على المجنى علية المتواجد فى خارج البلاد . وأكثر من ذلك يكفى أن يكون المراد بالتنظيم القيام بنشاط الاحتيال ، فلا يشترط أن يقوم أعضاء هذا التنظيم بالاحتيال بالفعل، ولكن يتعين أن يصدر من أعضائة أفعال مادية تتجة نحو الاحتيال على الغير لسلب أموالهم.

(ب) الغاية الربحية:

تتميز العصبة الاجرامية التى تقوم بالاحتيال عن الجرائم المنظمه التقليدية فى أن هذا الأخير يتسم باستعمال العنف أو التهديد به فى كثير من الأحيان بينما لا يعتمد نشاط العصبة فى حالة الاحتيال المنظم على العنف بل يعتمد على حمل المجنى علية على تسليم ماله اعتماداً على إقناعة وليس بناء على إستعمالة لوسائل تتسم بالعنف[1].

(جـ) استعمال شبكة الانترنت فى ارتكاب الجريمة .

يتميز نشاط عصابات الاحتيال لشبكة الانترنت فى الإيقاع بضحاياهم للاستيلاء على أموالهم فى حالات ليست بالقليلة.

---

(١) عبدالله سيف عبدالله سيف الشامى ، الجريمة المنظمة ، المرجع السابق ، ص ٧٣

الفصل الثانى

المشكلات القانونية المتعلقة بالاحتيال المنظم

ندرس فى هذا المبحث أهم المشكلات القانونية التى يثيرها الاحتيال المنظم ، منها ما يتعلق بوقوع هذا الاحتياتل عن طريق شبكة الانترنت ومنها ما يتعلق بمدى احترام المبادئ الأساسية فى القانون الجنائى، على سبيل بيانة.

المبحث الأول

أهم المشكلات القانونية المتعلقة بوقوع الاحتيال

عن طريق شبكة الانترنت

ارتبط ظهور شبكة الانترنت بازدياد فى جرائم الاحتيال سواء منها ما يقع من أفراد متفرقين أو من مجموعات عرضية أو من عصابات منظمة. من أهم تلك المشكلات القانونية ما يلى:

أولا- مدى وقوع الاحتيال بالدعاية الكاذبة على الانترنت:

كثير ما يقع الاحتيال بطريق الدعاية الكاذبة عن بضائع أو خدمات وهمية وأحياناً قد تكون هذة الدعاية صادرة عن أفراد أو شركات وهمية، فيثار التساؤل عن مدى إعتبار الدعاية على شبكة الانترنت داخلة ضمن الوسائل الاحتيالية.

تتجة التشريعات المقارنة فى غالبيتها الى تطلب وسائل احتيالية معينة للقول بتوافر جريمة الاحتيال(النصب)من أمثلة ذلك القانون الفرنسى (مادة ٣١٣ -١) والقانون المصرى (مادة ٣٣٦) والقانون الكويتى (مادة٢٣١) وقانون عقوبات، الاتحادى لدولة الامارات (مادة٣٩٩) وقانون العقوبات الأردنى (مادة ٤١٧) وقانون العقوبات البحرينى (مادة ٣٩١).

غير أن بعض التشريعات العربية توسعت فى مفهوم الاحتيال واكتفت

بتجريم الاحتيال دون تحديد صور معينة لهذا الاحتيال وبالتالى تترك الأمر لقاضى الموضوع لتحديد ما اذا كان النشاط الذى صدر من المتهم يشكل احتيالاً أو لا مثل قانون العقوبات القطرى وقانون العقوبات العمانى. فتنص المادة (٢٤١) من قانون العقوبات القطرى[1] على أنه "يرتكب جريمة الاحتيال كل من يخدع أو يغش أى شخص فيتوصل بذلك إلى : أ- تحقيق ميزة أو منفعة لنفسة أو لغيرة ب- حمل ذلك الشخص بسوء قصد على تسليم أى مال أو سند تعهد أو إبراء لأى شخص أو على أن يتخلى عن مال، أو جـ - أن يحمل قصد ذلك الشخص على أن يفعل شيئاً أو يمتنع عن فعل شئ ما لم يكن يفعلة، يعتبر إخفاء الوقائع بسؤ قصد خداعاً بالمعنى المقصود فى هذة المادة". وفى نفس الاتجاه تنص المادة (٢٨٨) من قانون العقوبات العمانى على أنه "يعاقب بالسجن من ثلاثة أشهر الى سنتين وبالغرامة .... من حصل من الغير على نفع غير مشروع أو للآخرين باستعمالة إحدى الطرق الاحتيالية .." دون أن تحدد المادة السابقة المقصود بالطرق الاحتيالية[2].

والأصل أن هناك فارقاً بين الدعاية الكاذبة كتجريم منفصل عن جريمة الاحتيال. فالدعاية الكاذبة فى حد ذاتها ليست من الطرق الاحتيالية، ولكنها تكتسب تلك الصفة فى حالة تدعيمها بما يوحى بالثقة عند المجنى عليهم. وبهذا قضت أحكام القضاء الفرنسى[3].

ولنا أن نتساءل عن اعتبار الدعاية على الانترنت من ضمن الوسائل الاحتيالية؟ من الجدير بالذكر أن الوسائل الاحتيالية كما تعددها التشريعات يدخل ضمنها المظهر الخارجى الذى ينطلى على الغير: فهل الدعاية على

---

(١) الصادر بالقانون رقم ١٤ لسنة ١٩٧١

(٢) د. غنام محمد غنام ، تجريم الكذب على المساهمين فى شركات المساهمة فى قوانين دول مجلس التعاون الخليجى، جامعة الكويت مجلس النشر العلمى ، ١٩٩٦ ، ص

(3) Crim. ١٠mai ١٩٧٨, Bull.crim. n ١٤٨, D.١٩٧٨, IR. ٣٤٨: Crim. ٥ juin ١٩٧٥, Bull.. crime . crim. . ١٤٦

الانترنت يمكن اعتبارها من الوسائل الخارجية التى من شأنها أن تقنع الغير بتسليم مالة؟ صدر للقضاء المصرى [١] والفرنسى [٢] أحكام أعتبر فيها الدعاية فى إحدى الجرائد المعروفة داخلة ضمن المظاهر الخارجية وبالتالى فإن أحكاما له انتهت إلى توافر الاحتيال إذا صدق المجنى عليهم تلك الدعاية وسلموا أموالهم لشركة غير جادة فى نشاطها وانتهى الأمر بها إلى الاستيلاء على أموال مودعى أموالهم فيها [٣].

بيد أننا نرى أن الاعلانات على شبكة الانترنت وهى شبكة ذات طابع دولى تختلف عن الصحف اليومية ذات الطابع المحلى ، يضاف إلى ذلك أن المصداقية على شبكة الانترنت أصبحت محل شك كبير لدى الشخص العادى، ومن ثم نرى أن مثل تلك الأحكام التى تعتبر النشر فى الصحف اليومية من قبيل الوسائل الاحتيالية فى جريمة النصب هى أحكام غير واجبة الإعمال إذا تعلق الأمر بشبكة الانترنت. وبناء علية نقول إن المجنى عليهم يجب أن يحترسوا عند مطالعة الإعلانات على شبكة الانترنت ، فلا يولوهم ثقتهم دون سبق التعامل مع الجهات التى تصدر عنهم. فإذا سلموا أموالهم دون أن يحتاطوا فإنهم يعتبرون مفرطين فى حق أنفسهم، ولا يحميهم القانون بوصفهم مجنى عليهم فى جريمة النصب.

والأمر يختلف إذا توافر من الظروف ما يدعو المجنى علية متوسط

(١) أنظر على سبيل المثال ١٣ديسمبر سنة ١٩٧٠ مجموعة أحكام النقض س ٢١ ص ١٢١١٢ رقم ٢٩٤

(2) Crim. ١٤mars ١٩٦٧, Bull.crim. n ١٠٢, Trib De la Roche du ١٣ janv ١٩٦٧ , ١ ,٣٠٢. crim ٢٨nov ١٩٦٨. Bull crim N 23[illegible]

(3) Renald [illegible] Le droit penal et la formation du contrat [illegible]

الحرص إلى تصديق الاعلان أو الدعاية كأن تكون صادرة كذباً عن جهة رسمية أو جهة محل ثقة الجمهور فيقدم الناس على تسليم أموالهم إلى صاحب هذا الإعلان المنسوب كذباً إلى تلك الجهة[1].

ثانيا – مدى وقوع الاحتيال على البنوك :

كثيراً ما يقع الاحتيال على البنوك وذلك من جانب أفراد وعصابات أحياناً تتخصص فى هذا اللون من الاستيلاء على الأموال باعتبار أن البنوك هى أكثر الجهات استهدافاً لتلك العمليات. ويرتبط بهذا اللون من النشاط صعوبات قانونية يتعين عرضها ومحاولة إيجاد حلول لها ؛ فهناك أولاً مشكلة مدى جواز الإحتيال الواقع على الآلة باعتبار أن الإحتيال يقع على كمبيوتر البنك فى شكل إيهامه بأن مصدر أمر التحويل مخول لإصدار هذا الأمر . وهناك مشكلة قانونية تتمثل فى الإجابة على التساؤل التالى: إذا التقط شخص ما بطاقة إئتمان تنتمى إلى شخص آخر واستخدم هذا الرقم لسحب مبالغ مالية من حساب صاحب البطاقة بدون وجه حق ، هل يعد ذلك من قبيل الوسائل الاحتيالية التى تشكل النظام فى جريمة الاحتيال (النصب) ؟

فى الإجابة على التساؤل الأول قضت القضاء فى غالبية التشريعات المقارنه بجوار الاحتيال على الآلة باعتبار أن الآلة أصبحت تحل محل الإنسان فى كثير من الأحيان وباعتبار أنه ليس فى القانون ما يستلزم أن يقع الإيهام على إنسان. من ذلك ما قضى به فى فرنسا من وقوع الإحتيال على كمبيوتر البنك ممن أعطى أمر تحويل من حساب شخص الغير باستخدام رقم

(١) د. غنام محمد غنام ، تجريم الكذب على المساهمين فى شركات المساهمة ، المرجع السابق ص ٣٥ .

بطاقة إئتمان خاصة بهذا الغير [١] وهو نفس الرأى الذى انتهت إليه محكمة التمييز الكويتية عندما قضت بأن استعمال المتهم لبطاقة السحب الذى يخص شخصاً آخر يكفى لوقوع جريمة النصب[٢]. ومع ذلك فإنه فى تشريعات أخرى لا تزال أحكام القضاء ترفض القول بأن الإحتيال يقع على الآلة ولا تزال تستلزم أن يقع الإيهام على إنسان وهذا هو الوضع فى كندا[٣] وفى الإجابة على التساؤل الثانى حول وقوع الاحتيال بطريق استعمال رقم بطاقة الائتمان التى يلتقطها أفراد وعصابات عن طريق شبكة الانترنت نرد بالايجاب على اعتبار أن استخدام الغير لرقم بطاقة الائتمان بدون اذن صاحبها من شأنه أن يوهم كمبيوتر البنك بأنه صاحب الحساب أو أنه وكيل عن صاحب الحساب عن هذا الاستعمال، ومن ثم بأن يمكن القول بأن هناك وسيلة احتيالية تتمثل فى استعمال صفة غير صحيحة ومن ثم يتوافر فى هذا الفعل وصف جريمة الاحتيال .

ثالثا -الاختصاص القضائي فى حالة الاحتيال الواقع عن طريق الانترنت:

إذا سلمنا بوقوع الاحتيال عن طريق الانترنت سواء عن طريق الاعلانات الكاذبة أو عن طريق أوامر التحويل بدون وجه حق، فإن هناك صعوبة قانونية تتعلق بتحديد المحكمة المختصة بسبب طابع شبكة الانترنت العابرة للحدود، فقد يبث المتهم الإعلان الكاذب أو يصدر أمر الإحتيال من بلد معين لإيهام شخص المجنى علية المتواجد فى بلد آخر(أو بنك يتواجد فى

(1) C.A. Paris nov. 1992, Juris – Classeur périodique, éd. Enterprice, 1994, n 357,p,252, n 15: Bordeaux 25 mars 1987,p. 424 note pradel

(٢) تمييز ٢٨/ ٥/ ٩٠ طعن رقم ٢٤٢ / ٨٩ جزائى، مجموعة القواعد القانونية التى أقرتها محكمة التمييز خلال الفترة من ١/ ١/ ٩٦ ، ص٦٩٢

(٣) د. شيماء عبدالغنى محمد عطا الله ، الحمايو الجنائية للتعاملات الالكترونية ، دار النهضة العربية ، ٢٠٠٨ ، ص ٦٢

دولة أخرى) فيقوم هذا الأخير بتسليم مال له إلى بنك المتهم الذى يتواجد فى نفس بلد هذا الأخير أو فى بلد ثالث. فهل يؤول الإختصاص بالتحقيق والمحاكمة إلى محاكم دولة المتهم أو دولة المجنى علية أو إلى قضاء دولة ثالثة يتواجد فيها البنك الذى تم تحويل المبالغ إلية؟

للإجابة على هذا التساؤل فى حالة وقوع جريمة الإحتيال يجب التذكير بأن المحكمة المختصة (وكذلك سلطة التحقيق المختصة) هى – وفقاً لمبدأ الإقليمية الذى يسود فى التشريعات المقارنة – هى محكمة المكان الذى وقعت فية الجريمة أو جزء منها [١]. وإذا طبقنا ذلك على جريمة الإحتيال نتذكر بأن تلك الجريمة من الجرائم المركبة[٢] ، حيث يتشكل فيها الركن المادى من نشاط ويتمثل فى ممارسة طريقة من الطرق الإحتيالية ونتيجة وتتمثل فى الإستيلاء على مال الغير وعلاقة سببية تتمثل فى إقناع المتهم للمجنى علية بتسليم ماله وحدوث هذا التسليم بناء على ذلك[٣]. وعلى ذلك فإن المحكمة المختصة بمحاكمة المتهمين فى جريمة الإحتيال هى تلك المحكمة التى مارس فى دائرتها المتهم النشاط الإحتيالى وكذلك محكمة المكان الذى تم فيه تسليم المال. غير أنه إذا تمت محكمة المتهم عن جريمة الإحتيال فى مكان من هذة الأماكن، فإنه لا يجوز إعادة محاكمته مرة أخرى عن ذات الواقعة وذلك لأنه لا يجوز محاكمتة شخص عن فعل واحد مرتين.

---

(١) وذلك بالإضافة الى معايير أخرى تتبناها بعض التشريعات كنظام الإجراءات الجزائية السعودى لسنة ١٤٢٢هـ وقانون العقوبات المصرى مثل مكان إقامة المتهم ومكان القبض على المتهم (مادة ١٣١ سعودى ومادة عقوبات مصرى) .

(٢) د. عبدالرؤف مهدى ، شرح القواعد العامة لقانون العقوبات ، ٢٠٠٧ ،ص ٣٨٤

(٣) د. فيصل عبدالله الكندرى ، د. غنام محمد غنام ، شرح قانون الجزاء الكويتى، القسم الخاص، الكويت ٢٠٠٦، ص ٤٤٦

بناء عليه فإنه إذا وقع الاحتيال بطريق شبكة الإنترنت، وقام المتهم بإرسال عروض احتيالية من بلد (أ) كما لو تعلق الأمر بإعلان كاذب مثلا في بلد (ب) فيرسل المبلغ المطلوب الي البلد (أ) او البلد (جـ) يكون في أحد بنوكها حساب للمتهم فيقيد المبلغ في حسابه هناك. في هذه الحالة يمكن القول بأن محاكم البلد (أ) تختص بمحاكمة المتهمين بهذا الاحتيال، كما تختص محاكم البلد (ب) بمحاكمة هؤلاء المتهمين. وحيث إن تسليم المال الذي هو يشكل النتيجة في الجريمة الاحتيال قد تم في البلد (ج) فإن محاكم هذا البلد الأخير تختص أيضاً بالمحاكمة في خصوص هذه الجريمة. وقد لاحظ البعض بأن جرائم الأنترنت يمر فيها عرض الاحتيال عن طريق الجهاز الخادم الذي قد يتواجد في أمريكا ومهمته تلقي العروض وتوزيعها علي جميع انحاء العالم، إذن فإن جزءا من الجريمة قد وقع في أمريكا أيضا مما يجعل المحاكم الأمريكية تختص بمحاكمة المتهمين أيضا بتلك(١). غير أن ذلك يشكل توسعة لا يوافق عليها الذوق القانوني السليم، لأنه يصعب تصور أن الولايات المتحدة الأمريكية يختص قضاؤها بمحاكمة المتهمين في جميع الجرائم التي تقع بطريقة الإنترنت، كما أن هذا القول يتعارض مع طبيعة عمل الجهاز الخادم الذي يتمثل في التوزيع التقني والتلقائي للرسائل التي يستقبلها وعدم القيام بدور حقيقي في تلقي العروض ومعرفة محتواها ثم إعادة توزيعها. فتوزيعها يتم بطريقة أتوماتيكية ولا تعكس أي دور في إتمام جريمة الاحتيال او غيرها؟؟؟ من الخادمة (السرفر) في المساهمة بدور فى إتمام جريمة الاحتيال او غيرها من الجرائم التي تقع بطريق الإنترنت(٢) .ومن الجدير بالذكر أن المحاكم فى

---

(١) د. شيماء عبد الغني عطاالله، المرجع السابق ص ٣٧٦.

2)) انظر في مسئولية مزودي الخدمات : د. شيماء عبد الغني عطاالله، المرجع السابق ص ١٦٤

التشريعات الأوروبية والأمريكية لم تقر بمسئولية مزودى الخدمات عما يقع من جرائم تتم بإرسال رسائل بطريق تلك الشبكة، نظراً لأن أجهزتهم تعمل بشكل تلقائى وأنه ليس لهم دور فى فحص الرسائل والتى لا تعد ولا تحصى، كما أن دورهم هو ليس دور القاضى، فلا يختص بالفصل فيما إذا كانت رسالة معينة تخالف القانون أو لا تخالفه ومن ثم فإنه يصعب إقامتهم رقيباً على ما تقوم شبكة الإنترنت ببثه، وإن كان هذا لا يحول دون إلتزامهم بتنفيذ ما يرد إليهم من أحكام أو أوامر قضائية بحذف رسائل معينة تخالف القانون أو تسبب ضرراً بحق الغيرة فى الخصوصية أو فى السمعة أو فى حق آخر يحمية القانون كالحق فى الأداء أو الحق على المصنفات الفنية والأدبية.

غير أن الرأى يختلف فى بعض جوانبه إذا أدخلنا تجريماً للجريمة المنظمة بطريق الإحتيال أى عاقب المشرع على الإنضمام لعصابه من أغراضها الإحتيال على الغير للإستيلاء على أموالة، لأن مجرد فعل الإنضمام إلى تلك العصبة يكون معاقباً علية دون إشتراط القيام الفعلى بالإحتيال على الغيرة، ومن ثم فإن المكان الذى تتكون فيه العصابة يصبح قضاؤة مختصاً بمحاكمة المتهمين، أما إذا مارس أعضاء العصبة إحتيالاً بالفعل، فإنهم يرتكبون جريمتين، الأولى هى جريمة تكوين عصبة إجرامية يكون من ضمن هدفها الإحتيال على الغير وجريمة الإحتيال على الغير. ومن المقرر فى غالبية التشريعات توقيع عقوبة الجريمة الأشد فى حالة توافر الإرتباط الذى لا يقبل التجزئة بين الجرائم[1]. فإذا كون المتهمين عصبة إجرامية يكون من غرضها الإحتيال وقاموا بالاحتيال فعلاً، فإن الجريمتين يتوافر بينهما ارتباط لا يقبل التجزئة، أما إذا كانت العصبة الإجرامية قد تكونت بغرض ممارسة أنشطة متنوعة مثل غسل الأموال والاتجار فى الآثار المهربة وكذلك الاحتيال، فإننا

(١) د. غنام محمد غنام ، شرح قانون العقوبات الاتحادى، مطبوعات جامعة الإمارات ، ٢٠٠٣ ، ص ٤٤٦

نرى أن حالة الارتباط الذى لا يقبل التجزئة لا يتوافر عندئذ وبالتالى فإن المتهمين يحاكموا عن كلتا الجريمتين وتوقع عليهم المحكمة عقوبتين باعتبار أن الأمر يتعلق بالتعدد البسيط للجرائم .

أما فى الولايات المتحدة الأمريكية فإنه منذ حكم المحكمة العليا سنة ١٩٣٢ فى معيار Blockburger قضى بأن التعديل الخامس ٥ th Amendment on doble jeopardy لا يحمى المتهم من تعدد العقوبات ما دامت كل جريمة تتضمن ركناً لا يدخل فى الجريمة الأخرى(١). وفى حكمها الصادر سنة ١٩٩٣ أكدت المحكمة ذاتها هذا الإتجاه وطبقته على استيراد المخدرات والتى قضت بصدده بأن الإدانة عنه لا تحول دون إدانة المتهم نفسة عن جريمة أخرى وفقاً لنص آخر وهى نقل المخدرات إلى داخل الولايات المتحدة بوسيلة من وسائل المواصلات. ولا يهم وفقاً لرأى المحكمة أن تكون الجريمة الأخرى داخلة كلية فى عناصر الجريمة الأولى(٢). وبالتالى فإن تعدد الجرائم جائز فى هذه الحالات فى القانون الأمريكى .

ومن الملاحظ أن الشريعة الإسلامية تترك أمر التعازير إلى ولى الأمر الذى له أن يتبنى هذا الأفكار وينص فى أنظمته على عدم العقاب مرتين عن جريمتين ما دام الإرتباط الذى لا يقبل التجزئة قد توافر بينهما. بل أنه فى حالة الحدود، إذا ارتكب المتهم جريمتين من جرائم الحدود ، فإنه لا يعاقب مرتين وفقاً لجمهور الفقهاء فى حالة الحدودالمتماثلة ما دام أن إرتكابة لجريمتين قد جاء قبل محاكمتة عن إحداهما(٣).

---

(١) Blockburger v U.S ٢٨٤U.S. ٣٠٤ ٩)١٩٣٢)

(٢) U.S.v. Florenz – pereza , ٥٨F. ٣d ١٦٤, ١٦٧)٥ th Cir. ١٩٩٥ ; (١١٦

(٥) عبدالقادر عودة ، التشريع الجنائى الإسلامى مقارناً بالقانون الوضعى ، دار التراث، الجزء الأول ، بدون تاريخ ٧٤٧

المبحث الثاني

مدى تعارض العقاب عن الاحتيال المنظم مع الحقوق الأساسية للمتهم

على الرغم من ارتكابة للجريمة فإن المتهم يتمتع بعدة حقوق، بعضها أساسى، بل إن بعضها منصوص علية فى الدستور. من هذه المبادئ مبدأ الشرعية ومبدأ عدم جواز محاكمة شخص مرتين عن فعل واحد، ومبدأ شخصية المسئولية ومبدأ التناسب ومبدأ ازدواجية التجريم، وضرورة احترام حرية الرأى والعقيدة ؛

(أ) مبدأ الشرعية:

يتمثل مبدأ الشرعية في أنه لا جريمة ولا عقوبة إلاّ بناء على قانون. ويترتب على ذلك نتائج هامة منها: ضرورة وجود نص في القانون أو لائحته تصدر بناء على قانون لتجريم مثل هذا الفعل. كما يترتب على مبدأ الشرعية ضرورة تحديد النص بشكل واضح يحول دون إبهامه أو إثارة الشكوك في التفسير حوله[1].

وإذا قرر المشرع أن يجرم فعل الاحتيال المنظم أو يدخل تجريما خاصا بالجريمة المنظمة جاعلا ضمن أغراضه ممارسة الاحتيال، فإن ذلك يجب أن يقترن باحترام مبدأ الشرعية في مضمونه سابق الذكر من حيث وجود النص ومن حيث وضوح النص على تجريم الاحتيال المنظم أو النص على الجريمة المنظمة التي من أغراضها ممارسة الاحتيال.

---

(1) د.غنام محمد غنام، شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة، المرجع السابق، ص ٣٠.

وتأتي المشكلة القانونية المتعلقة بمبدأ الشرعية من عدة أوجه:

أولا- هل يكفي في تجريم الانضمام إلى عصبة إجرامية تتخذ الاحتيال نشاطا رئيسا أو يدخل الاحتيال ضمن أنشطتها الرئيسة واقعة الانضمام دون استلزام أن يرتكب المتهم العضو فعلا يجعله فاعلا أو شريكا في الاحتيال؟ وتأتي تلك الخشية من موقف التشريعات المقارنة في خصوص العقاب على الجريمة المنظمة، فمن تلك التشريعات ما يكتفي بأن تشكل العصبة الإجرامية المنظمة دون اشتراط أن تقع أفعال إجرامية مادام أنها تكونت بقصد ارتكاب تلك الأفعال. ففي تلجيكا، ليس من الضروري للعقاب على الاشتراك في جماعة من البغاة association de malfaiteurs أن يثبت ارتكاب العضو لجريمة من تلك الجرائم التي أعدت العصبة لارتكابها[1]. ومن التشريعات ما يستلزم أن تقع أفعال مادية لارتكاب تلك الجرائم، أي أنه لا يشترط في جميع الأحوال أن تقع الجريمة تامة أي الاحتيال هنا.

ويتعلق بمبدأ الشرعية وضوح النص حيث يتعين إدراج حالات الاحتيال الخطيرة ضمن الجرائم التي تدخل ضمن أنشطة الجريمة المنظمة لكي يمكن اعتبارها ضمن الجريمة المنظمة. ولا يكفي في ذلك أن ينص المشرع على إدخال الغش ضمن تلك الأنشطة، ذلك أن تعبير الغش وإن كان صالحا في القانون المدني كعيب من عيوب الرضا التي من شأنها أن تدخل العقد قابلا للإبطال، وإن كان الغش يفسد كل شئ في القانون الإداري ويجعل القرار الإداري غير محصن من الإلغاء، فإن تعبير الغش لا يصلح في القانون الجنائي ، إلاّ إذا وصف بأنه الغش التجاري مع تحديد المقصود بهذا الغش كما تفعله

(1) Christopher L.Blakesely, The criminal justice system facing the challenge of organized crime, General report, preparatory colloquium, Alexandrie, nov. 8-12, 1977, International Review of Penal Law, 1998, p. 82.

القوانين المختلفة[1]، ومنها القانون المصري في شأن قمع الغش والتدليس بالقانون رقم ٤٨ لسنة ١٩٤١ المعدل بالقانون رقم ٢٨١ لسنة ١٩٩٤ والذي يعرف هذا النوع من الغش بقوله "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة ..... أو بإحدى هاتين العقوبتين كل من خدع المتعاقد معه بأية طريقة من الطرق في أحد الأمور الآتية في أحد الأمور الآتية: ١- ذاتية البضاعة إذا كان ما سلم منها غير ما تم التعاقد عليه. ٢- حقيقة البضاعة أو طبيعتها أو صفاتها الجوهرية أو ما تحتويه من عناصر نافعة ... ٣- نوع البضاعة أو منشؤها أو أصلها أو مصدرها.... ٤- عدد البضاعة أو مقدراها أو مقاسها أو كيلها أو وزنها أو طاقتها أو عيارها". ونفس الأمر يُقال بالنسبة لنظام مكافحة الغش التجاري في المملكة العربية السعودية الصادر في ٢٩/ ٥/ ١٤٠٤ هـ حيث تنص المادة الثانية منه على صور هذا الغش بقولها: المادة الثانية: يُعد مخالفا لأحكام هذا النظام كل من ١- خدع أو شرع في الخداع – بأي طريقة من الطرق في أحد الأمور التالية: ١- ذاتية المنتج أو طبيعته أو جنسة أو نوعه ... ٣- باع منتجا مغشوشا أو فاسدا أو عرضه... ٤- حاز منتجا مغشوشا أو فاسدا ٥- صنع منتجات مخالفة للمواصفات القياسية المعتمدة أو ..... ٦- استعمل آنية أو أوعية أو أغلفة .... ٧- عبأ منتجا أو حزمه أو ربطه أو وزعه أو ... ٨- استورد عبوات أو اغلفة .... ٩- استورد منتجا مغشوشا أو فاسدا".

وقد دفعت الخشية من مخالفة حقوق الإنسان إلى القول بضرورة وقوع فعل يعاقب عليه القانون حتى لا تصل إلى تجريم حالة وهي الانضمام إلى

---

(1) د. مجدي محب حافظ، موسوعة تشريعات الغش والتدليس، ١٩٩٨، ص ٩؛ د. عبد الحكم فودة، جرائم الغش التجاري والصناعي ، منشأة المعارف ١٩٩٦ ص ٣٣.

منظمة محظورة[1].

والواقع أن التشريعات تختلف في تجريمها لتكوين جماعة من البغاة association de malfaiteurs فالوضع في إيطاليا يختلف عما هو مقرر في فرنسا حيث يجب ارتكاب فعل إجرامي وفقا للقانون الفرنسي un fait materiel concrétisant la preparation du crime للعقاب على الانضمام إلى عصبة إجرامية بينما يكفي وفقا للقانون الإيطالي مجرد الاتفاق. لذا فإن فرنسا ترفض تسليم المتهمين بتلك الجريمة إلى السلطات الإيطالية بسبب اختلاف التشريعين من هذه الزاوية[2]. كما أنه بالنسبة لجريمة التآمر conspiracy وفقا للقانون الإنجليزي – يلزم ارتكاب فعل يرمي إلى ارتكاب الجريمة محل النشر[3].

ب) مبدأ شخصية المسئولية:

يثير تجريم الاحتيال المنظم مشكلات قانونية تتعلق بمبدأ شخصية المسئولية الجنائية حيث لا يجوز أن يُسأله شخص إلاّ عن فعله الشخصي. لذا يتنافر هذا النوع من المسئولية مع المسئولية عن فعل الغير. فإذا كانت المسئولية عن فعل الغير جائزة في القانون المدني، فإنها غير جائزة في مجال القانون الجنائي الذي تقرر في مجاله الدساتير المختلفة مبدأ شخصية المسئولية باعتبارها ضمانة من ضمانات الحرية الفردية. فالعقوبات الجنائية تتعلق بالحرية الفردية بشكل لا تتضمنه الجزاءات المدنية من تعويض أو فسخ العقد أو إبطاله.....

ومصدر الصعوبة بالنسبة للاحتيال المنظم أن قواعد الجريمة المنظمة

(1) Christopher L. Blakesley, id
(2) Marcel Leclerc, "La criminalité organisée, La documentation Française , 1996, p. 163.
(3) Christopher L.Blakesley,id p. 88

سوف تنطبق عليه، من هذه القواعد أن العضو في العصابة المنظمة التي تمارس الاحتيال ضمن أنشطتها الرئيسة سوف يُسأل عن هذا النشاط بصفته فاعلا أصليا حتى ولو لم يقم بفعل من الأفعال المادية للاحتيال في شكل إتيان جزء من الركن المادي أو حتى الشروع فيها. فسوف يكفي عندئذ أن تتجه نية أعضائها إلى الاحتيال حتى ولو لم يقع الاحتيال أو الشروع فيه (وتلك في التشريعات التي لا تستلزم وقوع فعل مادي للعقاب على الجريمة المنظمة). وتكتفي تشريعات أخرى بوقوع فعل مادي من أحد أعضائها يشكل احتيالا أو شروعا فيه أو حتى بالأعمال التحضيرية للاحتيال وذلك لمساءلة باقي أعضاء العصبة في تلك العصبة.

وقد وازن واضعو اتفاقية الأمم المتحدة للجريمة المنظمة لسنة ٢٠٠٠ بين مبدأ شخصية المسئولية ومبدأ المسئولية التضامنية لأعضاء الجريمة المنظمة ـــا تطلبت من المتهم العضو في الجريمة المنظمة لكي يُسأل عن جرائمها أن يصدر منه نشاط معين يتجه إلى ارتكاب الجرائم محل المسئولية. وقد أحسن واضعو الاتفاقية عندما حددوا (في المادة الخامسة) دور العضو المسئول دون أن يرتكب الجريمة ذاتها اكتفاء بارتكابه نشاط من الأنشطة التالية:

أ) أي من الفعلين التاليين أو كلاهما، باعتبارهما فعلين جنائيين متميزين عن الجرائم التي تنطوي على الشروع في النشاط الإجرامي أو إتمامه.

١- الاتفاق مع شخص آخر أو أكثر على ارتكاب جريمة خطيرة لغرض له صلة مباشرة أو غير مباشرة بالحصول على منفعة مالية أو منفعة مادية أخرى وينطوي ، حيثما يشترط القانون الداخلي ذلك، على

فعل يقوم به أحد المشاركين يساعد على تنفيذ الاتفاق، أو تكون ضالعة فيه جماعة إجرامية منظمة،

٢- قيام الشخص عن علم بهدف جماعة إجرامية منظمة ونشاطها الإجرامي العام أو بعزمها على ارتكاب الجرائم المعنية، بدور فاعل في : أ- الأنشطة الإجرامية للجماعة الإجرامية المنظمة، ب- أي أنشطة أخرى تضطلع بها الجماعة الإجرامية، مع علمه بأن مشاركته ستسهم في تحقيق الهدف الإجرامي المبين أعلاه.

ب) تنظيم ارتكاب جريمة خطيرة تكون ضالعة فيها جريمة إجرامية منظمة أو الإشراف أو المساعدة أو التحريض عليه أو تيسيره أو إسناد المشورة بشأنه.

ويتعلق بمبدأ شخصية المسئولية مدى جواز تقرير مسئولية الشخص المعنوي عن جرائم الاحتيال المنظم إذا اتضح أن شركة معينة كانت ستارا للقيام بأنشطة الاحتيال المنظم؛ فهل يجوز توقيع عقوبات معينة على هذا الشخص المعنوي؟ تردد الفقه التقليدي في القول بالمسئولية الجنائية للشخص المعنوي حتى أقرتها عديد من التشريعات مثل قانون العقوبات الفرنسي (مادة ١٢١-٢). وقد صرح قانون العقوبات الاتحادي في الإمارات بهذا المبدأ في المادة (٦٥) التي تنص على أن "الأشخاص الاعتبارية فيما مصالح الحكومة ودوائرها الرسمية والهيئات والمؤسسات العامة ،مسئولية جنائيا عن الجرائم التي يرتكبها ممثلوها أو وكلاؤها لحسابها أو باسمها ". وتكتفي تشريعات أخرى في بعض الجرائم بتقرير مسئولية الشخص المعنوي كالقانون المصري الذي أخذ بهذا النوع من المسئولية في صدد جرائم

غسل الأموال (مادة ١٦ من قانون مكافحة غسل الأموال رقم ٨٠ لسنة ٢٠٠٢).

وبناء عليه فإنه لم يصبح متعارضا مع مبدأ شخصية المسئولية أن يسمح المشرع بتوقيع عقوبات على الشخص المعنوي مادامت هذه العقوبات تتمشى مع طبيعة الشخص المعنوي مثل قفل المنشأة أو الحل أو وقف أو وقف النشاط أو الغرامة وذلك في حالة استخدام الشركة مثلا كستار للاحتيال على الغير والاستيلاء على أموالهم.

جـ مبدأ التناسب:

تتواجد هنا أمام صعوبة قانونية أخرى تتعلق بالتساؤل التالي: هل من سلطة المشرع أن يدخل الاحتيال ضمن الجريمة المنظمة أو أنه من الواجب عليه أن يراعي مبدأ التناسب أي أن الاحتيال ليس من الخطورة بحيث يكون متناسبا إدراجه في تلك الجريمة والتسوية بينه وبين تكون عصابة للاتجار بالمخدرات أو لغسل الأموال أو بالاتجار بالأعضاء البشرية أو بالرقيق الأبيض[1].

وأصبح من المقرر وفقا لتفسير المحكمة الدستورية في مصر أن على المشرع أن يراعي التناسب بين العقوبة وبين الجريمة، فلا يفرد عقوبة مغالى فيها لجريمة لا تستأهل تلك العقوبة بشكل واضح. وتعتبر المحكمة أن مخالفة شرط التناسب بصم القانون بعدم الدستورية استنادا إلى مخالفة مبدأ الشرعية.

---

(١) انظر في غسل الأموال :
Ahmed Farouk ZAHIR, Le blanchiment de l'argent et la recherche de produits de l'infraction, thèse , Nanted, 2001.

وقد أقرت المحكمة السابقة هذا المبدأ بقولها: "وحيث إن قضاء هذه المحكمة قد جرى على أن شرعية الجزاء- جنائيا كان أو مدنيا أو تأديبيا- مناطه أن يكون متناسبا مع الأفعال التي أثمها المشرع، أو حظرها أو قيد مباشرتها وأن الأصل في العقوبة هو معقوليتها، فلا يكون التدخل بها إلاّ بقدر لزومها ، نأيا بها أن تكون إيلاما غير مبرر يؤكد قسوتها في غير ضرورة، ولا يجوز بالتالي أن تناقض- بمداها أو طرائق تنفيذها – القيم التي ارتضتها الأمم المتحضرة مؤكدة بها ارتقاء حسها، تعبيرا عن نضجها على طريق تقدمها واستواء فهمها لمعايير الحق والعدل التي لا يصادم تطبيقها ما يراه أوساط الناس تقييما خلقيا واعيا لمختلف الظروف ذات الصلة بالجريمة"[1].

وقد تطرقت المحكمة الدستورية في حكمها إلى حدود سلطة المشرع عند التجريم وتقيدها بمبدأ الضرورة الاجتماعية بقولها:

"إن القانون الجنائي وإن اتفق مع غيره من القوانين في تنظيم بعض العلائق التي يرتبط بها الأفراد فيما بين بعضهم البعض، أو من خلال مجتمعهم بقصد ضبطها، إلاّ أن القانون الجنائي يفارقها في اتخاذ العقوبة أداة لتقويم ما يصدر عنهم من أفعال نهاهم عن ارتكابها، وهو بذلك يتغيا أن يحدد – ومن منظور اجتماعي- ما لا يجوز التسامح فيه من مظاهر سلوكهم، وأن يسيطر عليها بوسائل يكون فيها قبولهم اجتماعيا ممكنا. بما مؤداه أن الجزاء على أفعالهم لا يكون مبررا ، ذلك أن السلطة التي يملكها المشرع في مجال التجريم ، حدها قواعد الدستور، فلا يجوز أن يؤثم المشرع أفعالا في

---

(١) د. ممدوح عبد الحميد عبد المطلب، الاتجار بالبشر ، مجلة البحوث الأمنية، مركز البحوث والدراسات بكلية الملك فهد الأمنية، ٢٠٠٦ ص ٨٣.

غير ضرورة اجتماعية، ولا أن يقرر عقوبتها بما يجاوز قدرة هذه الضرورة"[1].

واستنادا إلى مبدأ التناسب في توقيع العقاب قضت المحكمة الدستورية في مصر – في ٢ يونيه سنة ٢٠٠١ [2]– بعدم دستورية المادة (٤٨) من قانون العقوبات التي كانت تنص – في فقرتها الأولى على جريمة الاتفاق الجنائي بقولها "يوجد اتفاق جنائي كلما اتحد شخصان فأكثر على ارتكاب جناية أو جنحة أو على الأعمال المجهزة أو المسهلة لارتكابها. ويعتبر الاتفاق جنائيا سواء أكان الغرض منه جائزا أم لا إذا كان ارتكاب الجنايات أو الجنح من الوسائل التي لوحظت في الوصل إليها". كما كانت تنص في فقرتها الثانية على أن "كل من اشترك في اتفاق جنائي سواء كان الغرض منه ارتكاب الجنايات أو اتخذها وسيلة للوصول إلى الغرض المقصود منه يعاقب لمجرد اشتراكه بالسجن. فإذا كان الغرض من الاتفاق ارتكاب الجنح واتخاذها

---

(١) المحكمة الدستورية ، جلسة ٤ يناير سنة ١٩٩٧ ، قضية رقم ٢ لسنة ١٥،

وقد رتبت المحكمة الدستورية على المفهوم السابق عدم دستورية قانون نقابات المهن التمثيلية والسينمائية والموسيقية بقولها عن ذلك القانون أنه :

"بعد أن حدد حصرا ما يخص كل منها من الأعمال المهنية التي قصر مباشرتها– أصلا– على المقيدين بجداولها ، عاقب بنص المادة ٥ مكررا غير أعضائها الذين يقحمون أنفسهم على نشاطها، دون تصريح منها يخولهم مباشرة بعض جوانبه، وكان التجريم –وباعتباره واقعا في هذه الحدود – يتناول في الأعم أعمالا إبداعية تمثل بمكوناتها عطاء دافقا ونهرا متجددا بعناصر الخلق التي تؤثر في بناء الفرد روحيا وعقليا، وكانت العقوبة التي فرضها المشرع على مباشرة هذه الأعمال دون تصريح بها هي الحبس والغرامة أو أحداهما – على الإطلاق – دون قيد يتعلق بالحد الأقصى لأيهما وإنمائها والحض عليها بكل الوسائل ، عملا بنص المادة (٤٩) من الدستور، ولأن الأصل هو جوازها لولا القيود المهنية التي فرضها التنظيم النقابي في شأنها – وهي بعد قيود ما كان ينبغي أن تصل وطأتها إلى حد إنفاذها من خلال جزاء جنائي يقيد الحرية الشخصية اعتسافا، مجاوزة بذلك قدر الضرورة الاجتماعية التي لا يجوز أن يكون بنيان التجريم منفصلا عن متطلباتها".

(٢) الجريدة الرسمية ، العدد ٢٤ في ١٤ يونيه سنة ٢٠٠١ ص ٩٢٦.

وسيلة للوصول إلى الغرض المقصود منه يعاقب المشترك به بالحبس".

وقد أكدت المحكمة في حكمها السابق على أنه "وحيث إن البين من استقراء نص الفقرة الأولى من المادة (٤٨) المشار إليها أنها عرفت الاتفاق الجنائي بأنه اتحاد شخصين أو أكثر على ارتكاب جناية أو جنحة أو على الأعمال المجهزة أو المسهلة لارتكابها، ولم يشترط النص عددا أكثر من اثنين لقيام الجريمة، كما لم يتطلب أن يستمر الاتفاق لمدة معينة أو أن يكون على قدر من التنظيم، وقد يكون محل الاتفاق عدة جنايات أو عدة جنح أو مجموعة جرائم مختلطة من النوعين معا. كما قد لا يرد الاتفاق إلاّ على جناية أو جنحة واحدة. ولم يستلزم النص أن تكون الجريمة أو الجرائم المتفق على ارتكابها على درجة من الجسامة، بل قد يكون محل الاتفاق اقتراف أي جنحة مهما كانت قليلة الأهمية في دلالتها الإجرامية، كنا أنه ليس بلازم أن تعين الجناية أو الجنحة محل الاتفاق كما لو تم الاتفاق، سواء كانت هذه الغاية في ذاتها مشروعة أو غير مشروعة، ومن ثم فإن نطاق التجريم جاء واسعا فضفاضا لا تقتضيه ضرورة اجتماعية مبررة".

وقد أكدت المحكمة في حكمها السابق على أن عقوبة الاتفاق هي السجن بينما يمكن أن يكون محل الاتفاق جناية يقضى فيها بعقوبة أخف من السجن. كما أن ع قوبة الاتفاق الجنائي هي الحبس إذا كان محلها ارتكاب جنحة، مع أن هناك من الجنح ما هو معاقب عليه بأقل من الحد الأقصى للحبس. ويدلل كل ذلك على عدم تناسب العقاب على الاتفاق الجنائي مع العقوبة المقررة بالإضافة إلى عدم بيان النص للركن المادي على وجه يقيني. وقد سبق أن اتجه كثير من الفقهاء إلى أن تجريم الاتفاق الجنائي هو محض خروج على قاعدة عدم جواز تجريم مجرد العزم على ارتكاب الجرائم[1].

---

(1) د. عبد الفتاح الصيفي، الأحكام العامة للنظام الجزائي ، جامعة الملك سعود، عمادة شؤون المكتبات ، ١٤١٦هـ.

ومن الواضح أن أفعال الاحتيال هي أعمال إجرامية، ومع ذلك فإنه من الواجب أن يكون الجزاء متناسبا مع الجريمة وأن يكون من الملائم النص على الاحتيال جنبا إلى جنب مع جرائم أخرى خطيرة مثل الاتجار بالمخدرات أو الاتجار بالرقيق الأبيض كمحل للنشاط في الجريمة المنظمة التي يصبح مقررا لها عقوبة ذاتها.

ويزيد من صعوبة الأمر أن التشريعات التي تعاقب على تكون عصبة إجرامية تستلزم درجة جسامة معينة في العقوبة وبعضها يحدد الجريمة التي تصلح محلا للعصبة الإجرامية. أما قانون العقوبات المصري، فإنه يعاقب على النصب بعقوبة الحبس (أي مدة لا تزيد على ثلاث سنوات) ويعاقب قانون العقوبات الإماراتي على الاحتيال في المادة (٣٩٩) بعقوبة الحبس (ثلاث سنوات في حدها الأقصى) أو الغرامة ونفس العقوبة الأخيرة يقررها قانون الجزاء الكويتي للاحتيال (مادة ٢٣٢).

أما قانون العقوبات الفرنسي فإنه في عقابه على تكوين جماعة الأشرار فإنه راعى خطورة الجريمة بنصه في المادة (٤٥٠-١) على أن "جماعة الأشرار هي مجموعة من الأشخاص تتشكل بغرض الإعداد بفعل أو بأكثر من الأفعال المادية لجناية أو أكثر أو جنحة معاقب عليها بالحبس مدة لا تقل عن خمس سنوات"[1]. ويلاحظ أن المشرع الفرنسي قد غاير في تعريف العصبة الإجرامية بين اعتبارها جريمة في حد ذاتها وبين اعتبارها ظرفا مشددا فيما يقع من جرائم أخرى. فعلى حين يستلزم أن تكون الجرائم محل نشاط

---

(1) "Constitue une association de malfaiteurs tout groupement formé ou entente établi en vue de la préparation caractérisée par un ou plusieurs faits materiels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonment" (Arrêt du 8 février 1979, Bull.Crim. N° 29, p. 67

العصبة الإجرامية كتجريم مستقل جنايات أو جنحا لا تقل في عقوبتها عن خمس سنوات، فإنه لم يستلزم مدة معينة من الحبس في حالة ما إذا كانت العصبة الإجرامية ظرفا مشددا في عقوبة الجرائم محل النشاط. فتنص المادة ١٣٢- ٧١ عقوبات فرنسي على أنه "يشكل عصبة إجرامية في مفهوم القانون كل تجمع من الأشخاص أو اتفاق الغرض من الإعداد- وذلك بفعل أو أكثر من الأفعال المادية – لارتكاب جريمة أو أكثر من الجرائم"(1).

وقد أكدت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة لسنة ٢٠٠٠ مبدأ التناسب عدما تطلبت خطورة الجريمة محل الإجرام المنظم واستلزمت (في مادتها الثالثة) أن يكون محل الجريمة المنظمة : ب) الجريمة الخطيرة حسب التعريف الوارد في المادة ٢ من هذه الاتفاقية، حيث يكون الجرم ذا طابع عبر وطني وتكون ضالعة فيه جماعة إجرامية منظمة. وقد عرفت الاتفاقية تلك الجريمة الخطيرة بقولها في المادة (٢) منها : ب) يقصد بتعبير "جريمة خطيرة" سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد".

د) مبدأ ازدواجية التجريم:

تثار أحيانا صعوبة قانونية بسبب وقوع الاحتيال المنظم عبر الدول فيقع الاتفاق على الاحتيال المنظم في بلد معين وتقع أفعال الاحتيال في بلد آخر فإذا كان هناك تنظيم على ارتكاب فعل معين في خارج البلاد، وكان هذا الفعل معاقبا عليه في ذلك البلد ولكنه غير معاقب عليه في البلد الذي المقصود ارتكابه فيه. فهناك من الأفعال ما يعاقب عليه القانون الوطني [illegible]

[illegible] bande organisé au sens de la loi tout groupement [illegible] en vue de la préparation caractérisée par un [illegible] matériels, d'une ou de plusieurs infractions".

ولا تعاقب عليها قوانين أخرى مثل إعطاء شيك بدون رصيد وإجهاض الحوامل وبعض جرائم أمن الدولة التي تتعلق بحرية العبير. فهل يلزم توافر شرط ازدواجية التجريم في هذه الحالة.

ومن ناحية أخرى قد يتوافر الفرض العكسي، عندما لا يكون فعلاً معينا معاقبا عليه في بلدنا حيث تأسس التنظيم محل الاتهام على أفعال لا تقع تحت طائلة التجريم ولكن للقيام بأفعال في خارج البلاد تعتبر جرائم وفقا لقانون العقوبات هناك. من ذلك أن يقوم المتهمون بتوزيع إعلانات كاذبة غير مدعمة بطرق احتيالية (وهو أمر تستلزمه كثير من التشريعات لوقوع جريمة الاحتيال وكان المجني عليه الذي وصل إليه الإعلان الكاذب متواجدا في بلد لا تستلزم توافر طريقة معينة من الطرق الاحتيالية كالمملكة العربية السعودية أو انجلترا): فهل يمكن مساءلة أعضاء التنظيم في هذه الحالة أو أنه يتعين قبول الدفع بانتفاء شرط ازدواجية التجريم الواجب توافره حيث ترتكب الجريمة عبر أكثر من دولة ؟

لا يمكن أن نذكر أن تأسيس عصبة إجرامية يجب أن يكون عن أفعال هي من الجرائم. والمقصود بالجرائم هي الأفعال التي يعاقب عليها البلد الذي يختص بمحاكمة المتهم. فإذا كان الفعل معاقبا عليه في حد ذاته (بوصفه احتيالا مثلا) وكان تأسيس جماعة إجرامية معاقبا عليه إذا كان محل نشاطها ذلك الفعل، فإن قانون تلك البلد ينطبق كما تختص محاكمها بمحاكمة المتهم بها. أما إذا كان الفعل الواقع خارج البلاد لا يشكل احتيالا ولكنه يكتسب هذا الوصف في القانون الوطني، فإن هذا القانون الأخير لا ينطبق على هذا التنظيم العصابي، كما لا يمكن مساءلة أعضائه عن هذا الفعل الواقع أو المزمع ارتكابه خارج البلاد، مادام أنه لم يكن معاقبا عليه في البلد الأجنبي.

وبالمثل فإنه لا يمكن مساءلة أعضاء التنظيم إذا كان الفعل محل التنظيم العصابي غير معاقب عليه وفقا للقانون الوطني حتى ولو كان معاقبا عيه وفقا لقانون البلد الذي وقع فيه أو مزمع ارتكابه فيه. ويبرز ذلك كله ضرورة احترام مبدأ ازدواجية التجريم في حالات الجريمة عبر الوطنية، مع ملاحظة أنه بالنسبة لبعض الجرائم لا يشترط توافر هذا المبدأ كما هو الحال في الجرائم التي تنتمي إلى مبدأ العينية (كجرائم تزوير العملة الوطنية وجرائم أمن الدولة وما يدخل فيها من جرائم الإرهاب) وكذلك الجرائم ذات الصبغة الدولية (مبدأ العالمية) كالجرائم ضد الإنسانية وجرائم الإبادة العرقية والجرائم الواقعة على المدنيين في أثناء الحرب (ويدخل قانون العقوبات الاتحادي الإماراتي وجرائم الاتجار بالمخدرات والرقيق الأبيض ضمن تلك الجرائم وفقا للمادة ٢١ منه). وبديهي أن جرائم الاحتيال لا تنتمي إلى تلك الطائفة من الجرائم الخطيرة التي يسري عليها مبدأ العينية أو مبدأ العالمية.

هـ) مبدأ عدم جواز محاكمة شخص واحد مرتين:

إذا حوكم المتهم عن جريمة محل نشاط العصابة الإجرامية كما لو ارتكبت العصابة احتيالا وكان القانون يعاقب على العضوية في تلك العصابة، فهل يجوز محاكمة الشخص مرتين: مرة عن الاحتيال الذي ارتكبته العصابة ومرة أخرى عن العضوية في تلك العصابة ؟ تجيب بعض التشريعات على هذا التساؤل بالإيجاب باعتبار أن الجريمتين مختلتين، فليس الوصف فقط هو المختلف ولكن الواقعة أيضا. واختلاف الواقعة لا ينشئ حجية للحكم المقضي به سواء صدر هذا الحكم من محكمة وطنية داخل البلاد أو من محكمة أجنبية. وبناء عليه تجوز محاكمته مرة أخرى. ولا يتصادم ذلك مع مبدأ عدم جواز محاكمة شخص عن فعل واحد مرتين.

ففي الولايات المتحدة الأمريكية هناك اختلاف بين تجريم conspiracy والجريمة الأصلية، إذن يرتكب المتهم جريمتين إذا تأخر على ارتكاب جريمة قم قام بارتكابها فعلا، وبالتالي لا يوجد في الأمر ما يخالف حظر المحاكمة المزدوجة double jeopardy [1]. وقد سبق القول بأن القانون الأمريكي لا يأخذ بفكرة الارتباط الذي لا يقبل التجزئة كمبرر لمنع تعدد العقوبات عند تعدد الجرائم. ويسمح القانون في ألمانيا بجواز محاكمة الشخص مرتين؛ مرة عن اشتراكه في عصبة إجرامية ومرة أخرى عن ارتكابه الجريمة التي اشترك فيها مع العصبة[2]. والحل الأفضل في هذه الحالة هو تطبيق قاعدة خصم العقوبة المقضي بها في الخارج.

وعلى العموم فإنه بالنسبة للجرائم التي حوكم عنها المتهم في خارج البلاد لا تعتد بعض التشريعات بتلك المحاكمة أو الأحكام الصادرة في خصوص المهم إلاّ إذا كانت هناك اتفاقية بين الدولتين بخصوص التعاون القضائي والاعتداد بالأحكام الجنائية الأجنبية. من تلك الدول ألمانيا وإيطاليا والنمسا. ومؤدى ذلك أنه تجوز محاكمة الشخص مرتين؛ مرة عن الاحتيال ومرة أخرى عن تكوين عصبة إجرامية لممارسة ذلك النشاط. على العكس من ذلك فإن هنا من التشريعات ما تعتد بأثر الحكم الأجنبي لكي ترتب عليه عدم جواز محاكمة الشخص مرة أخرى مثل هولندا وفنلندا. غير أن ذلك مشروط بوحدة الواقعة، الأمر الذي يتوافر في حالة تلك التهمتين[3].

وقد نصت اتفاقية شنجن Schengen الأوربية على أن " الشخص الذي تمت محاكمته نهائيا من جانب دولة متعاقدة لا يجوز ملا ملاحقته عن

---

(1) Christine, VAN DEN WYNGAERT, op.cit, p. 80
(2) Christine, VAN DEN WYNGAERT, op.cit, p. 81
(3) Christine, VAN DEN WYNGAERT, op.cit, p. 77

نفس الأفعال إذا تمت محاكمته. وفي حالة الإدامة تم تنفيذ الحكم عليه أو انقضى هذا التنفيذ وفقا لذلك القانون الأخير". وتضع المادة ٥٦ من اتفاقية شنجن مبدأ أن الدولة المتعاقدة يجب عليها أن تخصم مدة الحبس الذي نفذها المتهم في بلد آخر عن الجريمة ذاتها[1].

و) مخالفة حرية الرأي وحرية العقيدة:

من المحاذير التي تحيط بتجريم العضوية في عصبة يكون الاحتيال من ضمن أنشطتها ما يمكن أن يشكله هذا التجريم من مخالفة لحرية الرأي أو حرية العقيدة في بعض الأحيان بالنسبة لما تقوم به بعض الجمعيات الدينية من تجميع لأموال التبرعات من الجمهور بدعوى إنفاقها في أوجه الإحسان والصدقات على الفقراء والمحتاجين ثم يقومون بتوزيعها على أعضاء جمعيات دينية لأغراض مساعدتها على القيام بأنشطة معينة ذات صبغة سياسية، وقد تتلون في بعض التشريعات بلون ممارسة الإرهاب حيث تذهب تلك الأموال لكي تدعم أفراد تنظيمات سياسية وأسر المعتقلين لأغراض سياسية. ومن هنا كان من الضروري عدم استخدام هذا التجريم بغض تكميم الأفواه وإن اتصف بالمغالاة أحيانا، وفي نفس الوقت من الواجب عدم السماح باستخدام أموال الزكاة والصدقات في دعم الأنشطة المحظورة التي تشكل أفعالا للإرهاب أو إنشاء تنظيمات هدامة للنظام الاجتماعي أو السياسي (جرائم أمن الدولة من الداخل) أو في ارتكاب جرائم أمن الدولة من جهة الخارج.

AN DEN WYNGAERT, op.cit, p. 79

خاتمة ونتائج البحث

اتخذ الباب الثالث عنوانا له "طبيعة العلاقة بين الاحتيال والجريمة المنظمة في عصر الإنترنت" لكي يستكشف ظاهرة بدأت في الانتشار وهي وجود عصابات منظمة تمارس نشاط الاحتيال مستغلة التقنيات الحديثة التي تجعل الاتصالات عبر العالم سهلة ميسرة. والغاية واضحة والهدف جلي وهو حماية المجني عليهم من تلك العصابات التي تحمل المجني عليهم على تصديق مزاعمهم لكي تستولي على أموالهم.

وقد عالج هذا الباب الاحتيال كنشاط في الجريمة المنظمة وليس كجريمة فردية أو حتى جماعية ثم درس المشكلات القانونية التي تصطدم بالنص على تجريم منظم يكون الاحتيال من ضمن أنشطته الإجرامية.

وبعد الدراسة على الوجه السابق انتهينا إلى بعض النتائج وأهمها ما يلي:

- أصبح الاتجاه السائد في التشريعات المعاصرة هو النص على العقاب على الجرائم المنظمة على نحو مستقل عما ترتكبه العصبة المنظمة من جرائم.
- من اللازم تعريف الجريمة المنظمة بشكل ينفي الجهالة ويحترم مبدأ الشرعية وذلك بإيراد خصائصها وإيراد الجرائم التي قامت من أجل ارتكابها.
- من اللازم للعقاب على الجريمة المنظمة النص على ضرورة أن يرتكب بعض أعضائها أفعالا تشكل جرائم أو شروعا في جرائم، وذلك احتراما لمبدأ الشرعية حتى لا تسقط في عمومية النص وعدم

تحديده. فلا يكفي العقاب على تكوين عصبة إجرامية يكون الغرض منها ارتكاب أفعال مسهلة أو مجهزة لارتكاب الجرائم أن يرتكب أعضاؤها أفعالا مجهزة أو مسهلة لارتكاب الجرائم على نحو ما قضت به المحكمة الدستورية في مصر.

- إن التشريعات العربية لا تتجه بصفة عامة إلى النص على العقاب على الجريمة المنظمة إلاّ في مجال جرائم أمن الدولة على نحو ما يقرره قانون العقوبات المصري. وبدلا من ذلك فإن الاتجاه السائد في التشريعات العربية هو اعتبار الإجرام المنظم ظرفا مشددا في بعض الجرائم.

- إنه ليس من المناسب إدخال الاحتيال كنشاط من أنشطة الجريمة المنظمة التي يعاقب أعضاؤها على الانتماء إليها وذلك لأنه من المقرر وفقا لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة سنة ٢٠٠٠ ونظرا لأن التشريعات المقارنة تتجه إلى ضرورة أن تكون الجريمة منتمية إلى الجرائم الجسمية التي يعاقب عليها بالحبس مدة أطول عما هو مقرر بالنسبة للاحتيال. وبدلا من ذلك يمكن النص على إيراد ظرف مشدد للعقوبة في حالة ارتكاب الاحتيال من عصبة منظمة.

- من الواجب عند النص على العقاب على الجريمة المنظمة ضرورة احترام مبدأ الشرعية ومبدأ التناسب ومبدأ عدم جواز محاكمة شخص عن فعل واحد مرتين ومبدأ احترام حرية الرأي وحرية العقيدة.

مراجع البحث [1]

أولا – مراجع باللغة العربية :

(أ) كتب وأبحاث ومقالات :

- إبراهيم حامد طنطاوي ، جرائم العرض والحياء العام ، المكتبة القانونية ١٩٩٨ .
إبراهيم الدسوقي أبو الليل ، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة ، مؤتمر جامعة الإمارات العربية المتحدة ، كلية الشريعة والقانون حول " القانون والكمبيوتر والإنترنت " في الفترة ١ – ٣ سنة ٢٠٠٠ .
- أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، رسالة ، طنطا ، ٢٠٠ .
- أحمد شوقي الشلقاني ، الضرر في تزوير المحررات ، رسالة ، جامعة القاهرة ، ١٩٨٠.
- أحمد ضاعن السمدان ، " الحماية القانونية المدنية لبرامج الكمبيوتر " أعمال مؤتمر جامعة الكويت حول " القانون والحاسب الآلي " مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي ، ١٩٩٤ .
- إدوار غالي الدهبي ، الجرائم الجنسية ، ١٩٩٧ .
- جلال أحمد خليل ، النظام القانوني لحماية الاختراعات ونقل التكنولوجيا إلى الدول النامية ، مطبوعات جامعة الكويت ، مجلس النشر العلمي ، ١٩٨٣ .
- جميل عبد الباقي الصغير ، " القانون الجنائي والتكنولوجيا الحديثة " ، دار النهضة العربية ١٩٩٢ .
- الإنترنت والقانون الجنائي ، دار النهضة العربية ، ٢٠٠١ .
- حسام الدين كامل الأهواني ، " الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي ، أعمال مؤتمر جامعة الكويت حول " القانون والحاسب الآلي " مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي ، ١٩٩٤ .

(١) بترتيب أبجدي مع حفظ الألقاب

- سعيد عبد اللطيف ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت ، دار النهضة العربية ١٩٩٩

- سينوت حليم دوس ، تشريعات براءات الاختراع ، منشأة المعارف ، الإسكندرية ، ١٩٨٨ .

- عبد الرءوف مهدي ، شرح القواعد العامة للإجراءات الجنائية ، دار النهضة العربية ، ٢٠٠ .

- عبد العظيم مرسي وزير ، جرائم الأموال ، دار النهضة العربية ١٩٨٣ .

- علي عبد القادر القهوجي ، " الحماية الجنائية للبيانات المعالجة إلكترونيا " والكمبيوتر والإنترنت " مؤتمر " القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة ، مايو سنة ٢٠٠٠ ، المجلد الثاني .

- الحماية الجنائية لبرامج الحاسب ، دار الجامعة الجديدة ، للنشر ، ١٩٩٧ .

- عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، ١٩٩٥ .

- " لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات "بحث مقدم إلى مؤتمر " القانون والكمبيوتر والإنترنت ، مايو سنة ٢٠٠ ، الجزء الأول .

- " تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي " أعمال مؤتمر جامعة الكويت حول " القانون والحاسب الالي " ، مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي ، ١٩٩٤ .

- عمرو إبراهيم الوقاد ، الحماية الجنائية للمعلوماتية ، مجلة روح القوانين أبريل ١٩٩٨.

- غنام محمد غنام ، الحماية الجنائية لأسرار الأفراد لدى الموظف العام ، دار النهضة العربية ، ١٩٨٨ .

- عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ، بحث مقدم إلى مؤتمر " القانون والكمبيوتر والإنترنت " في الفترة من ١ - ٣ من مايو سنة ٢٠٠٠ .

- فايز عبد الله الكندري ، الحماية المدنية لبرامج الحاسب الآلي في القانون الكويتي ، في أعمال مؤتمر " القانون والكمبيوتر والإنترنت " ، جامعة الإمارات ، كلية الشريعة والقانون ، في الفترة من ١-٣ سنة ٢٠٠٠

- مراد رشدي ، الاختلاس في جرائم الأموال ، مكتبة نهضة الشرق ١٩٨٦.
- محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسب الإلكتروني ، دار الثقافة، ١٩٨٧ .
- محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ١٩٩٤ .
- المرجع العملي في الملكية الأدبية والفنية " ١٩٩٥
- محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي ، مطبوعات جامعة الكويت ، مجلس النشر العلمي ، ١٩٩٢ .
- " حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي " مطبوعات جامعة الكويت ، مجلس النشر العلمي ، ١٩٩٢ .
- محمود محمود مصطفى ، شرح قانون العقوبات - القسم الخاص ، دار النهضة العربية، ١٩٨٤ .
- محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ،دار النهضة العربية ١٩٨٨ .
- مصطفى كمال طه " القانون التجاري ، دار الجامعة الجديدة للنشر ، ١٩٩٠ .
- نزيه محمد الصادق المهدي ، الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية ، مؤتمر " القانون والكمبيوتر والإنترنت " جامعة الإمارات ، كلية الشريعة والقانون ، ١-٣ مايو سنة ٢٠٠٠ ، المجلد الأول .
- هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية ١٩٩٢ .
- " الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني ، مؤتمر جامعة الإمارات ، كلية الشريعة والقانون حول " القانون والكمبيوتر والإنترنت " ، في الفترة ١- ٣ مايو سنة ٢٠٠٠ ،

- هشام محمد فريد رستم ، " قانون العقوبات ومخاطر تقنية المعومات " مكتبة الآلات الحديثة ١٩٩٢ .

- الإتلاف العمدي لبرامج وبيانات الحاسب الإكتروني ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت "

- يعقوب يوسف صرخوه ، النظام القانوني للعلامات التجارية ، دراسة مقارنة ، جامعة الكويت ، مجلس النشر العلمي ، ١٩٩٢ – ١٩٩٣

(ب) أحكام القضاء :

- بني سويف الجزئية ، ١٧ نوفمبر سنة ١٩٢٠ المحاماة س ١ رقم ١٢٠ ص ٥٤٤

- نقض ١٨ أكتوبر سنة ١٩٤٣ ، مجموعة القواعد القانونية جـ ٦ رقم ٢٣٩ ص ٣١٦.

- نقض ١٢ مايو سنة ١٩٥٢ مجموعة أحكام محكمة النقض س ٣ رقم ٣٤١ ص ٩١٥ .

- نقض ٢٥ ديسمبر سنة ١٩٥٦ ، س ٧ رقم ٣٦٣ ص ١٣٢ .

- نقض ١٧ نوفمبر سنة ١٩٨٠ ، أحكام النقض س ٣١ رقم ١٩٤ ص ١٠٠٦.

- تمييز كويتي ٢٨ / ٥ / ١٩٩٠ طعن رقم ٢٤٢ / ٨٩ جزائي ، مجموعة القواعد القانونية التي قررتها محكمة التمييز خلال الفترة من ١/١/٩٦ ، ص ٦٩٢ .

- القضية رقم ٥٩ لسنة ١٨ ق. دستورية ، جلسة ١/٢/١٩٩٧ .

ثانيا – مراجع بلغة أجنبية :

(أ) كتب وأبحاث ومقالات :

- CBassiouni , " A draft International Criminal Code and Draft Statute for an International Criminal Tribunal , Martinus Nijhoff Publishers , Boston 1987 , p.439.
- Cahiers Lamy droit de l'informatique , Bulletin d'actualité, n° 89 fév. 1997.
- Guillaume CHAMPY, La fraude informatique , Presses Universitaires d'Aix - Marseille , 1992, p. 52

- Jim Drinkhall, Computer Fraud , Internet Fraud , Journal of Financial Crime , January 1997 , p. 258 .
- Cole Durham , The Emerging Structures of Criminal Information Law: Tracing the Contours of a new Paradigm , General Report for the AIDP- Colloquium, Delits informatiques et autres infractions à la technologie de l'information , Colloque préparatoire , Wurzbourg , Allemagne , Rev. Internationale de Droit pénal ,p. 100.
- Raymond GASSIN , " La protection pénale des informations sur la personnes en droit français contemporain" in " Droit pénal contemporain " Mélanges en l'honneur d'André Vitu , éd. Cujas 1989.
- Jacques FRANCIllON , " l'adaptation du droit pénal à certaines formes de délinquances informatiques et audio-visuelles " in " Droit pénal contemporain " Mélanges en l'honneur d'André Vitu , éd. Cujas 1989 .
- Jacques FRANCILLON , Les crimes informatiques et autres crimes dans le domaine de la technologie informatique en France , Rev. int. dr. pén. 1993, p.305.
- Jérôme Huet, Herbert Maisl, Droit de l'informatique et de télécommunications , Litec, 1989.
- Wilfrid JRANDIDIER, Interprétation de la loi pénale , Juris – class. pénal, Art 111 –2 à 111 – 5 , n° 38.
- Stanley Lai , Unauthorised use and section 1 of the Computer Misuse Act 1990 " , Journal of Financial Crime , May 1996, Vol. 3, N° 4 , p. 359.
- Eli Lederman , Computer Crimes and Other Crimes against Information Technology in Israel , Rev.int.dr.pén.1993,p.404.
- Xavier Linant de Bellefonds , Alain Hollande, Pratique du droit de l'informaftique, éd. Delmas 1989, p. 243.
- Marie- Paule LUCAS DE LEYSSAC, " Une information seule est-elle susceptible de vol ou d'une autre atteinte juridique aux biens ? " , D. 1985,chronique,43.
- Michel Margos, Michel Masse, Le droit pénal spécial né de l'informatique ,in " Travaux de l'institut de sciences criminelles de Poitiers, Informatique et droit pénal,", 1983.

- Manfred Möhrenschlager , Computer Crimes and Other Crimes against Information. Technology in Germany Rev.int.dr.pén.1993,p.338.
- K . Piragoff , Computer Crimes and Other Crimes against Information Technology in Canada , in " Délits informatiques et autres infractions à la technologie de l'information " , Rev. dr. pén. 1993, p. 206.
- Jean Pradel, Michel Danti- Juan, Droit pénal spécial, éd. Cujas , 1995,
- Michel – Laure Rassat, Droit pénal spécial, Dalloz, 1997, p.73 .
- Alan Reed, Peter Seago , Criminal law , ed. Sweet and Maxwell, 1999.
- James Richards," Transnational Criminal Organisations, Cybercrime , CRC Press , New York , Washington D. C. , 1999, p. 69 .
- Amanda Ryding, Management of Electronic Crime : Civil Aspects of Prevention and Containment, Journal of Financial Crime vol 6 N° 1 , August 1998, p. 56.
- Johm M. Scheb , John M. Scheb II , Criminal law & procedure , West / Wadsworth, third edition , 1999.
- Peter J. Schick , Gabriele Schmölzer , Comoputer Crimes and Other Crimes against Information Technology in Austria, in " Délits informatiques et autres infractions à la technologie de l'information " , Rev. int. dr. pén. 1993, p. 156.
- Ultrich Sieber, The international Handbook on Computer Crime, John Wiley & Sons, New York , 1986,
- J. C. Smith , The law of theft , seventh Ed. Butterworths, London, 1993 , p. 66 .
- Smith & Hogan, Criminal law , cases and materials ,Third edition ,Butterworths, London , 1986, p. 517.
- Jean P. Spreutels , Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Belgique , in " Délits informatiques et autres infractions à la technologie de l'information " , Rev. int. dr. pén. 1993, p. 163 .

- Travaux de l'Institut de sciences criminelles de Poitiers, Informatique et droit pénal , éd. Cujas , 1983 , p. 30 .
- John T. Soma , Thomas F. Muther Jr. , Heid M.L. Brissette, Transnational extradition for computer crimes; are new treaties and laws needed ? , Harvard Journal on Legislation , vol. 34, number 2, summer 1997, p. 348
- Université de Poitiers , Faculté de Droit et de Sciences sociales, " Les nouvelles pratiques délictuelles liées aux technologies de la communication " , Actes du Juriscope 96, Publication du Magistère en Droit de la Communicatique, P.U.F., 1999
- Michel Veron, Droit pénal spécial, Armond Colin', 1999, p. 197
- Vitu, Traité de droit pénal spécial , n° 1196 .
- Atsushi Yamaguchi, Computer Crimes and Other Crimes against Information Technology in Japan , Rev.int.dr.pén.1993, p. 437.
- Martin Wasik , Computer Crimes and Other Crimes against Information Technology in the United Kingdom , Rev.int.dr.pén.1993,p.629 .
- Edward M. Wise , Computer Crimes and Other Crimes against Information Technology in the United States , Rev.int.dr.pén.1993,p.657.

(ب) أحكام للمحاكم الأجنبية وتعليقات عليها :

- Crim 22 décembre 1955, B.C., n. 594.
- Trib corr. Auxerre , 10 décember 1963, G.P. 1964, I, 185, D.1964 Somm., 57.
- Warner (1970) 55 Cr. App. Rep. 93 .
- Crim. 9 juill. 1970, Bull. crim. n° 236; D. 1971, p. 3; J.C.P. 1971, II.
- 16616.
- Crim. 8 déc. 1971 , Bull.crim.,n° 341, p. 856.
- Ward v. The Superior Court of California (1972) .
- Arrêt Maillot, Crim. 7 nov. 1974 , Bull. crim. N. 323 , D. 1974 .somm. 144, Gaz.Pal.1975.I.somm.
- Crim. 11 oct. 1978, D. 1979, p. 76.

- Arrêt Giuesppe Sacchi , 30 avril 1979,Recueil de la jurisprudence de la Cour, p. 409.
- People v. Home Insurance Company (1979) .
- Arrêt U.C.I.P., Crim. 12 janv. 1981, Bull.crim.,n.15, p.58.
- Paris 4ème ch. A, 15 juin 1981, D. 1985.I. R. droit de l'informatique .p. 39.
- Trib Grande Inst. de Paris 10ème ch. , 9 mars 1982; Paris 4ème ch. A , 2 nov. 1982 ,
- Crim. 24 november 1983, D. 1984, 465 .
- R. v. Thompson, (1984) 3 ALL. ER 565. (1984) 79 Cr. App. Rep. 191 .
- Trib Grande Inst. de Paris, 3 ch. 27 juin 1984, I. R. droit de l'informatique, p. 39.
- R. v. Thompson, (1984) 3 ALL. ER 565. (1984) 79 Cr. App. Rep. 191 .
- Crim. 12 décembre 1984, Bull. Crim. 403, D. 25 avr. 1985, I. R. p. 186, Rev. sc. crim. 1985.
- Bouzat, Infractions contre les biens , Rev .sc .crim. 1985, chronique de jurisprudence ,p. 879.
- crim. 29 av. 1986, D. 1987. 131, Rev. sc.crim., 1987. 701 , Crim. 24 oct. 1990, Bull. n° 355,
- Crim. 9 mars 1987, J.C,P. 1988, II, 20913 .
- Bouzat , Infractions contre les biens, Rev.sc.crim 1987, chronique de jurisprudence, p. 211.
- Cour de Paris 24 juin 1987 , D. 1988. somm. 226 .
- Cour de Paris, Aff. Canal Plus, arrêt du 24 juin 1987 , Gaz. Pal. 1987 .2. 512, Rev .sc.crim.1987.p. 211.
- Trib. Gr. Inst. De Créteil 10 juillet 1987, D. 1988. J. 319.
- Cass. crim. 3 nov. 1987, D. j. 17, note Herbert Maisl.
- Bouzat ,Infractions contre les biens , Rev. sc. crim. 1987, chronique de jurisprrudence , p.211.
- Crim. 3 nov. 1987, comm. J. Frayssinet in Lamy, Droit de l'informatique, mise à jour 1988.
- Crim. 3 nov. 1987, Bull. crim. n° 382; Rev. sc. crim. 1988. 295, obs.
- Crim 3 nov. 1987 , D. 1988. J. 17, note Herbert Maisl.

- Crim 3 nov. 1987 , Bull. crim . n° 382 , rev. sc. crim. 1988. 295.
- Chan Man- Sin v. A.G. of Hong Kong (1988) 1 All Er, 1, (1988) Crim. L R 319.
- Crim. 12 janv. 1989, Bull.crim. n° 14 (arêt Bourquin) ,Gaz Pal. 1989.2. somm. 283, Rev. sc.crim.1990.507.
- Crim . 1er mars 1989 , Bull. Crim. n° 100.
- Crim 12 déc.1990, Bull.crim .n° 430, D. 1991. J. 364. Crim, 23 mars
- Rennes, 13 janv. 1992, D. 1993. Somm. 54 , obs.
- Crim. 3 mars 1992, Rev. sc. crim. 1993, p. 5461 .
- Crim. 3 mars 1992, Bouzat , infractions contre les biens , chroniques , Rev. sc. crim. 1993, p.546.
- Trib. Corr. Briey , 15 sept. 1992; D. 1994 . Somm. 289.obs. Maisl; Gaz. Pal . 1993 . I. 201 et la note , et 1994. I. Somm. 107 . 1992, B. n. 124 , 19 aout 1992 , B. n. 277, Rev. sc.crim.199
- Jacaues FRANCILLON, Infractions relevant du droit de l'information et de la communication, Rev.sc.crim. 1993, chronique de jurisprudence , p. 562.
- Cass. crim. 5 janv.1994; J.C.P. 1994. I. 359 , obs. Vivant et Le Stanc.
- Crim 5 janv. 1994, Gaz. Pal . 1996. somm. 419; 12 déc. 1996, Bull. crim. n° 465.
- Crim 1er janv. 1994, Dr. pénal , comm. 109.
- Agen, 28 fév. 1994, J.C.P. 1994. IV. 2209.
- Paris 5 avr. 1994, D. 1994. IR. 130 .
- Paris , 5 avr. 1994 , D. 1994, Flash , n° 18 .
- Crim. 19 janv. 1994, Rev.sc.crim 1994, p. 767.
- Paris 5 avr. 1994 , D . 1994 , IR. 130 ; comp. Douai 7 oct. 1992, Gaz. Pal.1993 .2.326, note Latry – Bonnart.
- Crim. 6 juill. 1994,cite par Jacaues FRANCILLON, " Infractions relevant du droit de l information et de la communication " Rev.sc.crim.1996, chronique de jurisprudence, p. 676.
- Reynald OTTENHOF, Infractions contre les biens, Rev.sc.crim. 1995, p. 820.
- Paris 15 mars 1995: J.C.P. 1995, IV. 1425 .
- TGI. Marseille , 23 mars 1995, D. 1996 , 40 , note Frayssinet.
- Crim. 3 avril 1995 J.C.P. 1995. II. 22429, Gaz, Pal. 24, 25 mai 1995, Rev. sc. crim. 1995, 599, Crim.26 oct. 1995, Bull. crim.n. 324, Rev. sociétés 1996, p. 326.

- Crim 25 oct. 1995, Bull.crim.n° 320 ; Rev. sc. crim. 1996, note Mole; Dr. pénal 1996. Comm. 86, note Véron .
- Jacques FRANCILLON," infractions relevant du droit de l'information et de la communication,",Rev. sc. crim. 1995 ,Chronique de la jurisprudence , p. 602.
- Crim 19 déc. 1995; Bull. crim. n° 387; Rev. sc. crim.1996. 679, obs. Francillon ; Dr. pénal 1996. comm. 126, note Véron ; D. 1996. IR. 81.
- Paris 13 sept. 1996. 677, obs. Francillon ; Dr. pénal 1996, 32, obs Véron .
- Aix – en – Provence, 23 oct. 1996, Gaz Pal . 1997. 2. 489, note Latry – Bonnart ; Rev. sc. crim. 1998. 140, obs Francillon .
- Trib. corr. De Paris 5 nov. 1996, Cahiers Lamy droit de l'informatique Bulletin d'actulité, n° 89 fév. 1997, p. 9 et 10 .
- Reynald OTTENHOF , Infractions contre les biens, chronique de jurisprudence, Rev.sc.crim.1996,p.658.
- Crim. 12 déc. 1996, Bull . crim. n° 465; Rev. sc. crim. 1998, obs. Francillon ; RTD com. 1997. 521; Gaz, Pal . 16 – 17 avr. 1997, cour
- TGI , Lille , 18 déc. 1996; D. 1997, 373 .
- Cour d'appel de Paris 14 janvier 1997, Cahiers Lamy droit de l'informatique, Bulletin d'actualité, n° 97, nov. 1997, p. 12.
- Crim. 4 mars 1997, Bull crim. n° 83; Rev. sc. crim. 1997, 669, obs. Dintilhac; J.C.P. 1997.IV.1612; Dr. pénal 1997. Comm. 75 , note Véron .
- Trib. correc. De Thionville , 3 juin 1997 , Expertises, n° 208, oct. 1997, p. 317. obs Bertrand.
- Corr. Poitiers , 26 juin 1997; Gaz. Pal . 1997, chron. 215, Rev. sc. crim. 1998, 145.
- T. corr. Mans , 16 fev. 1998, in " Responsabilité pénale d' un utilisateur : détournement d un ordinateur à usage professionnel pour récéler des images pédophiles , J. C.P. 1999. II. 10011.
- Crim. 8 déc. 1998, Bull. crim. n° 335; Jacques FRANCILLON , " Infractions relevant du droit de l'information et de la communication" , Rev. sc. Crim. 1999, chr. 606.

الفهرس

الموضوع	الصفحة

الموضوع	الصفحة

الموضوع	الصفحة

الموضوع	الصفحة
سابعًا: إفشاء أسرار المعلومات الشخصية	١٢١
المبحث الثاني: ضرورة توفير الحماية الجنائية لنظام الكمبيوتر	١٢٤
- ضرورة استحداث نصوص خاصة لحماية المعلومات داخل الكمبيوتر	١٢٤
- المعلومات داخل الكمبيوتر جديرة بالحماية عن المعلومات الورقية	١٢٤
المطلب الأول: تجريم التداخل في نظام الكمبيوتر	١٢٥
- الاتجاه إلى تجريم مجرد التداخل في التشريعات المختلفة	١٢٥
- طبيعة الجريمة: التداخل جريمة نشاط	١٢٧
- الركن المادي في جريمة التداخل	١٢٨
- النشاط الأول: الدخول في النظام	١٢٨
المقصود بالدخول	١٢٨
المقصود بالنظام في جريمة التداخل	١٢٩
- عدم الرضا عنصر في الدخول المؤثم	١٣٠
- عدم تجريم الدخول وفقا للقواعد العامة	١٣٠
- اختلاف التداخل عن اعتراض الرسائل المرسلة بطريق الكمبيوتر	١٣٢
- اختلاف التداخل في النظام عن استعماله	١٣٥
وسائل الدخول في النظام	١٣٦
أ تشغيل كمبيوتر مقفول	١٣٦
ب الدخول إلى كمبيوتر عن طريق خط تليفوني	١٣٧
حـ الدخول إلى كمبيوتر من كمبيوتر آخر	١٣٨

الموضوع	الصفحة
د- الدخول إلى نظام متصل بنفس الكمبيوتر	١٣٩
د- التجسس على النظام	١٤٠
- تجريم بعض التشرعات لمحاولة التدخل	١٤١
- النشاط الثاني : البقاء في النظام بعد الدخول عرضا إليه	١٤٢
- اختلاف جريمة التداخل عن جريمة البقاء في الطبيعة القانونية	١٤٤
- الركن المعنوي	١٤٥
- الظروف المشددة في الجريمة	١٤٦
المطلب الثاني : تجريم إعاقة نظام الكمبيوتر أو الإخلال بسيره	١٤٧
- الركن المادي	١٤٧
١- الإعاقة	١٤٧
٢- الإخلال بسير النظام	١٤٨
- الركن المعنوي	١٤٨
- الركن المعنوي	١٤٨
- تطلب القصد الجنائي	١٤٨
- حماية الاكتفاء بالقصد المتعدي	١٥٠
المطلب الثالث : تجريم العبث بالبيانات المبرمجة	١٥١
- الركن المادي	١٥١
- الركن المعنوي	١٥٣
المبحث الثالث : ضرورة الأخذ في الاعتبار الوضع الخاص باستعمال الانترنت في ارتكاب الجرائم	١٥٤
المطلب الأول : استخدام شبكة الانترنت في ارتكاب الجرائم	١٥٥

الموضوع	الصفحة

الموضوع	الصفحة
- مدى حق مأموري الضبط القضائي في الإطلاع على محتوى الرسائل	١٧٩
الفصل الثاني : ذاتية إجراءات التحقيق في مجال جرائم تقنية المعلومات	١٨٥
- مدى وجوب صدور إذن قضائي لاعتراض أو تسجيل المحادثات الالكترونية	١٨٥
- وجوب صدور إذن قضائي للدخول إلى البريد الالكتروني	١٩٠
- حالات تفتيش واعتراض المراسلات والبريد الالكتروني	١٩٢
أولاً :- اعتراض وتفتيش المراسلات والبريد الالكتروني بناء على إذن قضائي	١٩٢
- الجهة المختصة بإصدار إذن تفتيش الكمبيوتر	١٩٣
ثانيًا : جواز تفتيش الكمبيوتر استنادًا إلى الرضاء	١٩٧
- صحة التفتيش الصادر صاحب النظام	١٩٧
- صحة التفتيش الصادر من رب العمل	١٩٨
- توافر الرضا المفترض استنادًا إلى التحذير عن وجود مراقبة	١٩٨
ثالثًا : اعتراض وتفتيش الاتصالات الالكترونية بناء على حالة التلبس	١٩٩
- ذاتية إجراءات الضبط في مجال الجريمة الالكترونية	٢٠٢
الفصل الثالث : ذاتية إجراءات المحاكمة في مجال جرائم تقنية المعلومات	٢٠٣
المبحث الأول : الطابع الخاص للاختصاص القضائي في مجال جرائم تقنية المعلومات	٢٠٤
- الطابع الدولي لاختصاص المحاكم في جرائم تقنية المعلومات	٢٠٤
- تحديد المحكمة المختصة وفقا للقواعد العامة	٢٠٥
المبحث الثاني : الطابع الخاص للمستندات الالكترونية كدليل في الإثبات أمام المحكمة	٢١١

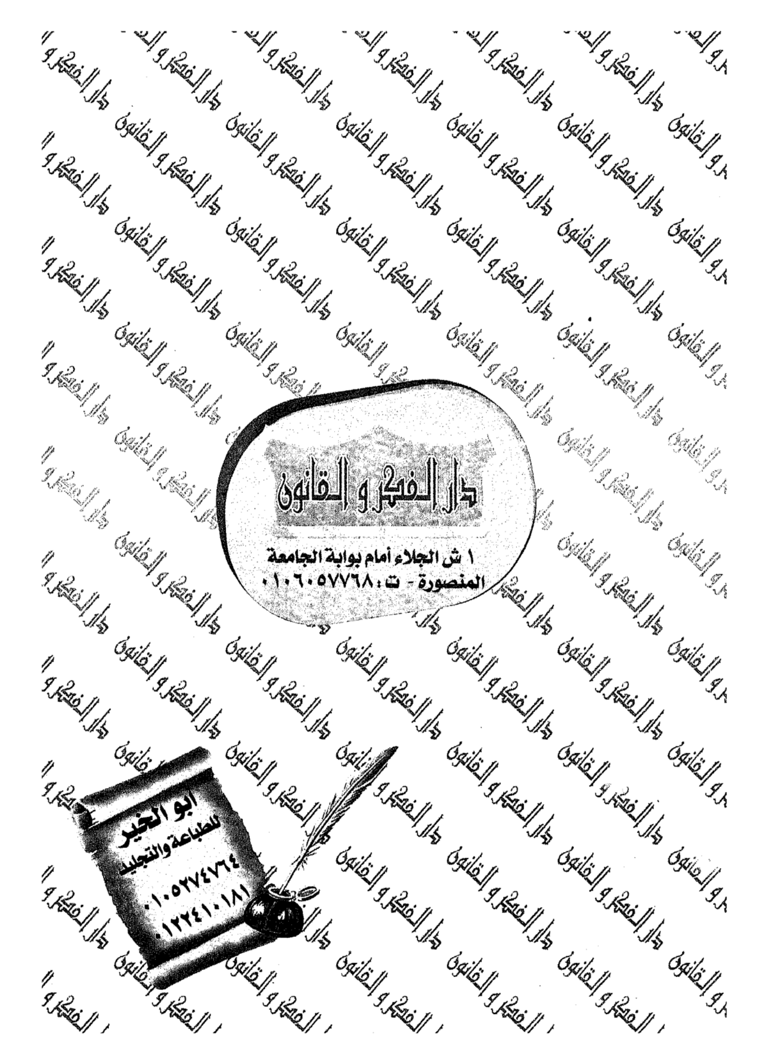
الموضوع	الصفحة

الموضوع	الصفحة

الموضوع	الصفحة

دار الفكر و القانون

١ ش الجلاء أمام بوابة الجامعة
المنصورة - ت : ٠١٠٦٠٥٧٧٦٨



دار الفكر و القانون
١ ش الجلاء أمام بوابة الجامعة
المنصورة - ت: ٠١٠٦٠٥٧٧٦٨
ابو الخير
للطباعة والتجليد
٠١٠٥٢٧٤٧٦٤
٠١٢٢٤١٠١٨١

